

InfoDOMAIN

DECISION SUPERIORITY FOR THE WARFIGHTER

SUMMER 2009



FLEET ELECTRONIC WARFARE CENTER
CHANGING THE FACE OF COMBAT

FEATURES

- 3 **My Domain**
CAPT Brian Hinkley explains NETWARCOM's Fleet EW Center
- 6 **NETWARCOM SOYs represent Leadership**
Twelve Domain Sailors journey to Vlrginia for 2009 selection board
- 7 **AWG accelerates Shipboard Accreditations**
NAVSTA Mayport ships complete iT21 systems accreditations
- 8 **NETWARCOM Sailors set Awards Standard**
A Bronze Star winner, as well as individual & unit language awardees
- 16 **Sailors from two NIOCs remember Shipmates**
Misawa & Hawaii memorial services for EC-121 crew
- 18 **Satellite & Network Performance at Sea**
Navy's Internet Protocol Effort increases Abilities at Sea
- 21 **NCDOC Commander added to Federal 100 List**
FCW magazine selects CAPT Petty to be part of its 2009 list
- 22 **Navy Network Security 101**
Do's and Don'ts of keeping the Navy's computer networks secure
- 26 **NETWARCOM's new Fleet EW Center**
Changing the face of combat, while enhancing the Fleet
- 29 **Navy Network & OPSEC Blunders**
Blue & Red Teams, as well as OPSEC share security tips
- 34 **NCTAMS LANT DET Bunswick, ME**
Tactical Support Communications Center prepares for closure
- 35 **Meet Northeast Base Communications Officer**
NWS, Earle, NJ 's BCO has been supporting command for 28 years
- 39 **AFCEA selects 30 Copernicus Awards in '09**
Littoral Combat Ship Sailor named for Web accomplishments
- 40 **NCTAMS LANT DET Cutler, ME**
New Insulators keep antenna system up & running

DEPARTMENTS

- | | |
|----------------------------|---------------------|
| 5 Force Chaplain | 10 Short Circuits |
| 12 Letters from the Ground | 15 Cyber Warrior |
| 30 Navy Reserves | 36 NGEN Update |
| 42 Team Spotlight | 46 People Spotlight |
| 48 Special Recognition | 50 Diversity |

OUR COVERS: Graphic Illustration by MC2 Travis K. Burcham. For more information about the Fleet EW Center, see pages 26-28.

EDITOR's NOTE: A photo caption (Spring 2009), had a Sailor as belonging to NCTAMS LANT, when in fact he was aboard USS ABRAHAM LINCOLN.



Commander, Naval Network Warfare Command
VADM H. Denby Starling II

Vice Commander
RADM Edward H. Deets III

Deputy Commander
Mr. Terry Halvorsen

Public Affairs Officer
LCDR Doug Gabos

Editor
Mr. George D. Bieber

Associate
MC2 Travis K. Burcham

Visual Information Specialist
Mr. Robin D. Hicks

Production
Quintessential Color Group
Upper Marlboro, MD

InfoDomain is the professional magazine of Naval Network Warfare Command that promotes the advancement of Information Operations, Intelligence, Networks and Space through an open exchange of better practices, tactics, current strategies and future strategies in order to meet the global challenges of the information warfare domain.

Information contained in *InfoDomain* does not necessarily reflect the official views of the U.S. Government, the Department of Defense or the Department of the Navy. Editorial content is prepared by the Public Affairs Office of Naval Network Warfare Command.

Articles for publication in *InfoDomain* should be submitted through the appropriate command representative. Security and policy review must be completed by submitting commands before submissions can be considered for publication. Address all correspondence to Editor, *InfoDomain*, Naval Network Warfare Command, Naval Amphibious Base Little Creek, Public Affairs Office, 2465 Guadalcanal Road, Norfolk, VA, 23521-3228; telephone (757) 417-7958 ext. 5, DSN 537-7958 ext. 5, FAX (757) 492-8702. Comments or queries may also be forwarded via e-mail to george.bieber@navy.mil

I want to thank you for the opportunity to tell you about our tremendous team of Electronic Warfare (EW) and Spectrum experts at the Fleet EW Center (FEWC) and our critical mission within Naval Network Warfare Command (NETWARCOM). Our EW and Spectrum control efforts are concentrated under the N3 Operations Department because of the direct and significant operational impact of EW/Spectrum capabilities and readiness on our fleet, and we continue to work closely with the other directorates within NETWARCOM to ensure enhanced fleet readiness for EW and Spectrum manning, training and equipping issues.

As a result of substantial research and analysis into Fleet EW/Spectrum challenges, the Fleet Commander recently released a naval message that announced NETWARCOM's establishment of the FEWC, and also established a new, separate EW Fleet Collaborative Team (FCT), chaired by VADM H. Denby Starling II, commander NETWARCOM, and assisted by three Flag-level leads, to leverage the valuable pockets of EW expertise across the many platforms and domains in the Fleet.

The role of the FEWC is to (1) consistently maintain visibility and current, accurate information on EW and Spectrum challenges, (2) perform the management functions required to enable the EW FCT to resolve deficiencies and to advise the Fleet Commander through VADM Starling, and (3) act as the fleet's EW/Spectrum "DC Central" to provide thoroughly coordinated answers to emergent requirements from higher echelon commanders. We also



provide for operational control of the Navy and Marine Corps Spectrum Center to handle operational spectrum issues in the electromagnetic battlespace across the globe.

FEWC plank owners consist of a brilliant cadre of professionals, including an outstanding officer corps: CDR Pat "Meeso" Honeck, an EP-3 pilot, and LCDR Chris "Tread" Saufley, an EA-6B Electronic Countermeasures Officer (ECMO); a tremendous senior enlisted team with Surface Warfare expertise: CTTCMs Thomas Wellman and Bob Marcotte and CTTC Jon Thomas; and expert civilian Spectrum advisors: Chuck "I trained Tiger" Tabor and Deems Wiggs. The team is supported by a top-notch contractor team consisting of Booz Allen Hamilton's Bob Stuart, former CO, Fleet Information Warfare Center (FIWC), Doug Persons, Steve Lubawski, Andy Rigazzi, and Tom "IO's in my name" Bascio; EW Associates: Dan Roper, former CO, USS ENTERPRISE (CVN 65) and Mark Caren, former CO, USS LA SALLE (AGF-3); and Dynamic Analytics and Test (DA&T): Tony Marra and team. Rounding out our team are experts across the Fleet including invaluable support from Steve Mervyn, Naval Surface Warfare Center, Crane, IN, and Dennis Gronseth and Tony Redes, Navy Information Operations Center (NIOC) Norfolk. We dedicate our efforts daily in memory of a fellow plank holder and shipmate, the late ETCM (SW/AW) Al Andrews.

Why all the concern about EW?

The demand for a focus on EW is greater than ever before. Our ability to control the increasingly contested EMS at the time and place of our choosing will determine our ability to influence and defeat adversaries in future conflicts. Recent events, including combat operations in Iraq and Afghanistan, have highlighted EW capacity and capability challenges in support of joint commanders around the globe. These challenges have direct application to our ability to perform Navy missions.

Has EW become the face of combat in the Information Age?

EW is almost a limiting term. I would say that "Electromagnetic Spectrum (EMS) warfare" is a more appropriate term for the face of combat or better yet, the "battle space" of the Information Age. The EMS runs through all warfighting domains including undersea, surface, land, air, space and cyber, and is a critical asset used by each of our platforms. To effectively prepare for future combat operations, the Information Warfare, Information Professional, Intelligence and Unrestricted Line (URL) communities will need to leverage each others' expertise better than we have in the past. The outcomes of future battles will depend on our ability to control the spectrum in order to control information flow, both ours and that of our adversaries.

Why should the Navy be taking the lead in solving EW deficiencies?

The Navy has always maintained a strong core of EW professionals and has an impressive track record of tactical and operational EW successes over the past several decades

and in combat today. Challenges in Electronic Warfare are definitely a problem facing all services and Joint operations, but the Navy has a unique skill set that can offer its experience and expertise to the Joint fight. The Navy has chosen to be proactive in re-examining our current construct to address internal EW challenges first. Our developments may be useful to other services in the future. Further, the Navy can be very proud of its investment in EW capabilities and capacities to date. We are widely recognized as the leading service for our commitment for programmatic improvements across the Future Years Defense Plan. The EA-18G Growler, Next Generation Jammer, and the Surface Warfare EW Improvement Program (SEWIP) are all tremendous examples. Our continued investment in EW keeps the Navy at the forefront of leading EW developments in the future.

How did your particular background contribute to the Fleet's focus on EW, how was the EW Way Ahead concept for the Fleet developed and why was development centered at NETWARCOM?

In 2005, the CNO initiated action to apply EW expertise as a unique Navy skill set to contribute to the Joint fight in Iraq. I was fortunate enough to have been given the opportunity to be the first commander of that action as Commander, Joint CREW (Counter Remote-Control Improvised Explosive Device Electronic Warfare) Composite Squadron ONE (JCCS-1). Since then, the Navy has sent hundreds more EW qualified Sailors to Operation Iraqi Freedom and Operation Enduring Freedom with the end result being a significant measurable success against a formidable Radio-Controlled improvised Explosive Device (RCIED) threat. This successful application of EW into the fight highlighted the positive impact that EW could have on the battlefield, and just as importantly, how lack of EW capability could impair our combat capability.

The Director of the Navy Staff (DNS), VADM John C. Harvey Jr., recognizing the potential benefits for additional EW focus, contacted Commander, NETWARCOM, and created the unprecedented opportunity for an O-6 with a Navy EW background at NETWARCOM to look holistically at EW as a warfighting capability across domains, not limited by any specific platform or program.

NETWARCOM, already assigned as the Information Operations Type Commander, was doctrinally responsible for EW. Further, being an Echelon III command, NETWARCOM was ideally situated to engage directly with the Fleet, while being responsible to directly report to the Fleet Commander. Finally, 3-star flag leadership gave the renewed focus on EW the clout and legitimacy required to have a direct, positive impact. These reasons and more convinced leadership to create the NETWARCOM Fleet EW Center.

Is the FEWC the new Navy Center of Excellence for EW?

No, not really. As opposed to there being one Navy EW

AT A GLANCE

CAPT Brian E. Hinkley is currently leading the Fleet Electronic Warfare Center (FEWC) within NETWARCOM, focused on Fleet EW readiness. He was commissioned through the U.S. Naval Academy in 1983. He was designated a Naval Flight Officer in November 1984 and headed to Whidbey Island, WA to begin his EA-6B "Prowler" carrier aviation career.

After completing Electronic Countermeasures Officer (ECMO) training at the EA-6B Fleet Replacement Squadron (FRS), Hinkley joined Tactical Electronic Warfare (VAQ) Squadron 135 "Black Ravens" for his first sea tour in October 1985. Cruising aboard USS CORAL SEA (CV-43) and then aboard USS ENTERPRISE (CVN 65), he participated in combat strikes over Libya and against Iranian naval forces. Following his first shore tour, serving as an FRS instructor, he earned a master's degree in Financial Management at the Naval Postgraduate School, Monterey, CA.

Hinkley served on Carrier Group FOUR staff as the Space and Electronic Warfare Officer. He returned to Whidbey Island for his department head tour with the VAQ-141 "Shadowhawks" serving as Maintenance and then Operations Officer, flying combat missions over Bosnia-Herzegovina from USS THEODORE ROOSEVELT (CVN 71). He also completed shore tours in Washington, DC, as the EA-6B junior officer detailer and then as Joint Chiefs of Staff European Command J6 Liaison Officer.

He served as Executive Officer and then assumed command of VAQ-135, deploying on USS CARL VINSON (CVN 70) and USS NIMITZ (CVN 68), where he flew combat operations in Operation ENDURING FREEDOM over Afghanistan immediately after Sept. 11, 2001, and supported Operation IRAQI FREEDOM over Iraq in 2003. Selected for major command at sea in 2005, he completed Naval Nuclear Power School and Nuclear Prototype Training, and then served as Deputy Director, Naval Aviation Enterprise Total Force Readiness.

In 2006, Hinkley screened for major command ashore and was selected to create and become the first operational commander of Joint CREW Composite Squadron ONE (JCCS-1) at Camp Victory in Baghdad, Iraq, leading the Navy effort to enhance EW capabilities within the U.S. Army and U.S. Marine Corps during Operation IRAQI FREEDOM.

During his naval aviation career, Hinkley accumulated more than 2,700 flight hours and 600 carrier landings.



FORCE CHAPLAIN'S THOUGHTS

In an operational environment, whether it is a routine deployment or an IA assignment, service members face various kinds of stresses and potential injuries. While physical wounds are the most visible, there are unseen emotional, psychological, spiritual or moral injuries Sailors may experience that go unnoticed and -- even worse -- untreated.

All injuries, whether physical or mental, effect the service member and his family. When people are physically ill, they usually don't hesitate to get medical care. Additionally, there is no stigma associated with someone who is physically injured seeking medical attention.

However, this is not always the case when a person experiences a psychological, emotional, spiritual or moral injury. Some people might even question whether a person who suffers from an unseen injury really needs professional care. These factors contribute toward psychologically injured people being less prone to ask for help.

Some common sources of stress injury include: a life threatening event, the wear and tear of operational fatigue, grief and moral conflict. The Navy is making a concerted effort to encourage service members to receive the help they need with these kinds of injuries.

Several programs have been established to make mental health support more available and remove the stigma associated with receiving it. The Warrior Transition Program gives IA's information about symptoms of psychological problems and where they can receive assistance, if needed. There is a wide range of other resources. Military OneSource is available 24/7 and can be reached at 800-342-9647 or at www.militaryonesource.com.

They will make an appointment for you to get help from a mental health professional outside of the Navy. Chaplains, Navy medicine, and Fleet and Family Support Center counselors are other resources you or your family can use. If you have any of unseen wounds, help is available, and you owe it to yourself and your family to get it.

May God Bless,

CAPT George Adams, USN

... continued on Page 25



(Right) RADM Edward H Deets III, deputy commander, NETWARCOM, joins the domain's 2009 SOY candidates for a group photo at Sheraton Waterside in downtown Norfolk, VA. (Center, front row) YN1 Kimberly Ferguson, NIOC Georgia received the Shore SOY honor and (on RADM Deets' right) CTI1(AW/NAC) Erich Keough, NIOC Misawa, Japan, was chosen as Sea SOY.

NETWARCOM SOYs represent Deckplate Leadership

Story & photo by MC2(SW) Christopher J. Koons

Naval Network Warfare Command (NETWARCOM) honored five domain Sailors of the Year (SOY) at a ceremony aboard Naval Amphibious Base Little Creek in March.

CTI1(AW/NAC) Erich Keough of Navy Information Operations Command (NIOC) Misawa, Japan, was chosen as Sea SOY, while YN1 Kimberly Ferguson of NIOC Georgia received the Shore SOY honor. The Reserve SOY award went to EN1(SW) Michael Watson of Joint Mobile Ashore Support Terminal Aurora, CO.

"I feel very honored to have won," said Watson. "It's a humbling experience. We do our job every day to support the Navy. It's great that those around us recognize what we do."

ET2(SW) Samuel Renfrow of Naval Computer and Telecommunications Area Master Station Pacific was named Junior Shore SOY, and CTR1(SW/AW) Anna Nichols of NIOC Georgia, who won the award before she advanced to petty officer first class, was named Junior Sea SOY.

"I couldn't have done it without the support of my junior Sailors and the guidance of my senior leadership," added Keough. "I say 'thank you' to all of them."

"We had some great competition," Ferguson said. "I'm thankful to have had the chance to spend this past week with these other first class petty officers and to be able to take the information I learned from them back to my command."

During the week leading up to the ceremony, the SOY candidates were each interviewed by selection boards made up of senior enlisted NETWARCOM Sailors. They also networked with each other, participated in physical fitness training together, toured local museums, attended receptions in their honor and enjoyed a dinner cruise around Norfolk Harbor.

"I loved the camaraderie amongst all the candidates," said IT1(SW) G.J. Jones of NCTAMS PAC Hawaii, last year's Shore SOY winner who was being considered for a second award. "We all came together, with everyone here completely dedicated to the Navy. We're all 'grade A' Sailors."

"I learned different leadership and motivational techniques from the other candidates," added CTR1(SS/SW) Ryan Astle of NIOC Maryland, who was competing for Sea SOY. "Everyone here realizes that how their junior Sailors perform is their most important concern."

The Sailor of the Year candidates are all role models for junior Sailors to emulate, according to NETWARCOM Force Master Chief (SS/AW/SW) Charles Dassance.

"These Sailors represent the base of deckplate leadership," said Dassance. "The positive impact they have made on the lives and careers of the young Sailors around them is truly inspirational."

Other NETWARCOM Sailor of the Year candidates were: CTI1 Anthony Bolouri-Rad of NR NIOC Georgia; CTR1(SW/AW) Patricia Acevez of NIOC Suitland, MD; CTR1(SG/SW) Ryan Astle of NIOC Maryland; CTT1(SW/AW) Jerome Hughs of NIOC Georgia; IT1(SW) G.J. Jones of NCTAMS PAC Hawaii; CTI21(SW) Brian Waggoner of NIOC Texas and IT1(SW/AW) Mark Watson, NCTAMS Naples, Italy."

Afloat Working Group accelerates Shipboard Computer Accreditations

By MCC(SW/AW) Aaron Strickland

JACKSONVILLE, FL -- An Afloat Working Group (AWG) led by Naval Network Warfare Command (NETWARCOM) and the Navy's Certifying Authority, also from NETWARCOM, assisted 22 Information Assurance Managers (IAMs) from 12 Naval Station Mayport ships in completing accelerated Information Technology-21 (IT21) system accreditations in April.

The working group spent five days in Jacksonville, providing on-scene assistance to shipboard IAMs in completing their IT21 system accreditations.

The collaboration produced results - well ahead of what previously would have taken six months, according to Jean Simmons, Fleet Forces Command Certification and Accreditation leading reviewer, assigned to NETWARCOM's chief information office.

"You can't ask for better results than that," Simmons said. "This process is expected to be the way forward for fleet accreditation in the future."

IAMs pored over computers loaded with the paperwork necessary to achieve the Certification and Accreditation (C&A) each ship needs to connect to the Navy's Global Information Grid (GIG) of computers and information networks overseen by NETWARCOM. C&A means the ship has met Defense of Department requirements for confidentiality, system integrity, authentication, non-repudiation and availability, according to NETWARCOM's Designated Approving Authority (DAA).

According to Simmons, the accreditation is a milestone each ship must complete, and it must be updated at least every three years once the ship has received authorization to operate.

As they moved through their checklists, IAMs shared information on how their ships are equipped. Simmons said that information sharing was vital in speeding up the accreditation process.

The results were so quick that the commanding officers and executive officers of two participating ships were hesitant to sign the completed documents, but were assured by Simmons that a thorough evaluation had been performed.

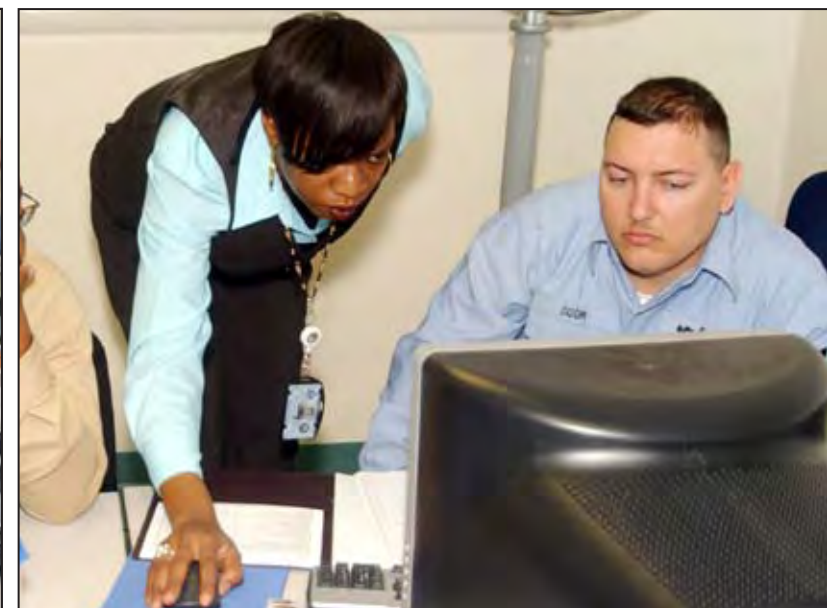
Simmons said the AWG was being watched closely by officials throughout the Navy. She expects similar groups to meet at other Navy fleet concentration areas such as Norfolk, VA and San Diego.

"It felt good to see all the ships accredited at one time instead of a long, drawn-out process that would take time, lots of e-mails and mean lots of corrections," Simmons added. According to her, the Afloat Working Groups' appeal is the time that has been saved by bringing the C&A Working Group and the IAMs from different ships together.

"We can explain the process, explain the documents, and show them what they're doing right, show them their mistakes and fix them on the spot," Simmons concluded.



(Left to right) ITC(SW) Marcus Walton and IT1(SW/AW) Carlos Ortiz discuss their assignment during the Fleet Forces Command Certification and Accreditation Afloat Workshop held for Sailors assigned to ships located at Naval Station Mayport. (Photo by MC2 Elisha Dawkins)



(Left to right) Jean Simmons assists IT1(SW) Vernon A. Doom during the Fleet Forces Command Certification and Accreditation Afloat Workshop. This workshop is being held for Sailors assigned to ships located at Naval Station Mayport. (Photo by MC2 Elisha Dawkins)

NIOC Hawaii's Bronze Star Sailor

By CTI2 Theresa M. Buitron, NIOC Hawaii

HONOLULU -- CTR2 Edwin Cordero, an individual augmentee (IA) previously assigned to Naval Information Operations Command Hawaii, was recently awarded the Bronze Star Medal for exceptionally meritorious service during Operation Iraqi Freedom.

Cordero was assigned to an IA billet in Iraq soon after his reenlistment in July 2007. After three months of training, he spent the next seven months in Iraq as a member of the Joint Expeditionary Signal Tactical Reconnaissance detachment where he was able to see other aspects of the intelligence world, as well as the Army side of the force.

"I learned a lot out there. While working on this assignment, I got to see the effectiveness of intelligence out in the field," said Cordero. "For anyone who doesn't realize it, what gets done at shore commands is important and it greatly affected what we did."

Cordero worked with the 101st Airborne team on the ground, and they earned his respect.

"Working the tactical side was completely different than being behind a desk," said Cordero. "I was running around Baghdad, working perimeter patrols. It was sort of like being a cop."

Overall, Cordero said his experience was eye-opening and that he was able to learn about the fast paced tempo of the Sailors and Soldiers in that environment.

"We were always on the move; there were a lot more thinking-on-your-feet situations. However, it was also very satisfying to see the results of our work right away," he said.

Cordero joined the Navy in November 2003, just a few

months after graduating from high school. He grew up in the Bronx, and when the attacks of Sept. 11, 2001 occurred, he wanted to go into the service right away.

Although he originally wanted to go into the Marines, the Navy ended up being a better fit for Cordero as he wanted to work with computer systems. He considered the Cryptologic Technician - Maintenance field,

but being a Cryptologic Technician (Collection) proved to be a better job. It gave him the opportunity to experience his work in Hawaii and also the IA assignment to Iraq.

After just six months of being back in the states, Cordero is now getting ready to ship out again, this time on a West PAC tour aboard the USS Nimitz (CVN 68).

"I'll be out for about 6-7 months again, however, this tour will probably be a piece of cake compared to working in Iraq. And, this time I get port calls," remarked Cordero. "I'm also thinking about staying in for 20 years. Maybe I'll work toward becoming an officer."



CTR2 Edwin Cordero on patrol in Iraq.

Photo by CTR2 Daniel Comant

Vela selected NETWARCOM Linguist of the Year

From NIOC Maryland Public Affairs



Official U.S. Navy Photo

CTI1 Julio Vela

CTI1 Julio Vela, who previously was recognized as NIOC Maryland's 2008 Language Professional of the Year, has been selected as Naval Network Warfare Command's Language Professional of the Year and the Department of the Navy Language Professional of the Year. He will now compete at the Department of Defense level.

In his nomination letter, Vela was cited as an unmatched linguist, a consummate professional whose language abilities, technical expertise and leadership have proven invaluable to the success of the warfighter in combating violent extremism.

Vela was deployed for 96 days in support of a unique and highly competitive Chief of Naval Operations-sponsored program.

There he provided outstanding assistance to two squadrons and he led and trained a five-person joint service team under arduous conditions.

While not on deployment, Vela was requested by name to support a requirement in his area of expertise. His contributions made an immeasurable impact within the community to include national-level policy making and real-time support to forward-deployed forces.

He also expanded his professional development by completing the Aviation Maintenance Rating non-resident training course (a pre-requisite for Enlisted Aviation Warfare Specialist), six graduate level courses and was certified as a Command Financial Specialist.



NIOC Maryland's Command Language managers. (Photo by CTI1 Paul Goeth)

NIOC Maryland garners DoD Language Award

By MCSN Caymen Santoro, NIOC Maryland

Naval Information Operations Command (NIOC), Maryland recently received the Department of Defense Language Program of the Year Award for 2008, becoming the first Navy command to receive this honor in the history of the award.

This award follows the fourth consecutive year that the command has won the RADM G. P. March Foreign Language Excellence Award and the Department of the Navy Language Program of the Year.

The DoD award is presented annually to a military command for having achieved superior linguistic readiness and demonstrating the deepest commitment to linguists' professional development.

"NIOC Maryland is dedicated to the creation and maintenance of an innovative language program that provides high quality language instruction and guidance to its Sailors," said CTIC Heather Stokes, Command Language Program Manager (CLPM). Stokes and the NIOC Maryland Foreign Language Advisory Group (FLAG) have established a dynamic program that challenges linguists to continually improve and strive toward excellence.

"NIOC Maryland is committed to the quality investment that must be made in its linguists for continued development of a highly competent linguistic workforce," said Stokes. "The success of our program is attributed to aggressive efforts in optimizing training opportunities in order to satisfy fleet and operational requirements."

Others who supported this program include Assistant CLPM, CTI1 Christopher Oshlo, former Assistant CLPM CTIC Kristin Scott and members of the FLAG.

According to NIOC Maryland Commanding Officer, CAPT Richard Bodziak, "Being selected as the DoD's Best Language Program is a significant milestone, and one that we can all be proud of. From a larger

perspective, it validates all the hard work put in by Chief Stokes and her team of professional linguists," he said. "It also confirms the Navy's focus on improving readiness each and every day and being prepared to answer all bells."



(Right) ENS Michael Schmidt discusses his display with CTICS Gina Rivera at NIOC Maryland's Cultural Fair at McGill Training Center. (Photo by CTI1 Paul Goeth)

Cyber Readiness Key to Mission Success

By Dan Bowen, Commander Fleet Activities Yokosuka Public Affairs

YOKOSUKA, Japan -- The Defense Information Systems Agency (DISA) will be on board Commander Fleet Activities Yokosuka (CFAY) in June to conduct a command cyber readiness inspection (CCRI).

Inspectors will look into several areas to assess CFAY's ability to maintain the integrity of its portion of the global information grid (GIG).

According to www.globalsecurity.org, "the GIG represents a globally interconnected, end-to-end set of information capabilities and processes for collecting, processing and managing information on demand to warfighters, policymakers and support personnel. The GIG fulfills a fundamental principle of network-centric operations by securely connecting people and systems regardless of time or place, providing vastly superior situational awareness and better access to information for accelerated decision-making."

What this means to CFAY personnel is that with the GIG in place, a threat to one user is a threat to all users. The inspection will look at physical security, network

assurance, information awareness and will also determine if there are any deficiencies in the system.

According to LT Michael Gann, Naval Computer and Telecommunications Station Far East (NCTSFE) department head, who will serve as the military lead for the CCRI at NCTSFE, everyone has a part to play in maintaining system integrity.

"Little things go a long way in protecting our networks," said Gann. "Don't wear security badges outside of your spaces; make sure you don't allow interlopers into your secure spaces, and don't leave your common access card (CAC) unattended in your computer. Also, know who your security manager is and follow the rules concerning information assurance and physical security."

Users also need to be aware of visiting unauthorized Web sites, opening suspicious e-mails and sending secret information over the Non-Secure Internet Protocol Router Network (NIPRNET).

Protecting the network is not limited to classified networks only.

Adversaries to the United States look for ways to breach cyber security and gain access to systems and information. Information doesn't have to be classified to potentially have a significant negative impact to the nation's overall defense posture. Bits of unclassified information can be pieced together and allow adversaries to make clear estimations and logical deductions concerning the classified information.

Additionally, the Navy uses the unclassified networks for logistical support of deployed units worldwide. Exploitations of these networks could be the difference between "click" and "bang." Therefore, protecting the NIPRNET is as vitally important as protecting classified networks.

"Your work computer is a tool, same as a government vehicle, a needle gun or a weapons system," said Gann. "Use it correctly or it will be taken away. All it takes is one guy [to use the computer improperly] to bring down the entire network." ❧

NMCI GAL gains access to other Services via JEDS

From NMCI Public Affairs Office

ARLINGTON, VA -- The Navy Marine Corps Intranet (NMCI) has now reached a new level of interoperability and integration for its users, simply by connecting them with their counterparts across the Department of Defense. A new Enterprise Global Address List will allow NMCI users to find people in the other branches of the military from their desktops.

This spring, NMCI is rolling out a new Global Address List (GAL) that synchronizes NMCI with the Defense Information Systems Agency's Joint Enterprise Directory Services (JEDS). JEDS houses the contact information for personnel in the Army, Air Force, Coast Guard, Marine Corps, Navy Bureau of Medicine & Surgery (BUMED), and the Integrated Shipboard Network System

as well as other Defense agencies.

Microsoft Outlook users will be able to search all DoD address books, or narrow their search by selecting a specific agency's address book. Once a contact is found, users will be able to easily add that individual to their contacts.

CAPT Scott Weller, program manager for NMCI, said, "This new GAL will allow for greater collaboration between our enterprises and the DoD community, a key component of the Department of the Navy's Maritime Strategy."

Current DoD directory services do not support interoperability between services, which makes emails and contact information in those directories inaccessible

to the larger DoD community. DoD directive 8500.1 instructed the services to become net-centric by integrating all DoD information directory services.

NMCI is the first defense IT network to meet the requirements of the DoD directive.

The roll-out of the new GAL will reach all NMCI users by the end of the summer. Users will receive a user alert approximately two days prior to their scheduled installation.

To receive the new GAL, users must be logged onto their computer, but not necessarily Outlook. If users are logged into their Outlook inbox, they will receive a warning requiring them to close Microsoft Outlook. Once

closed, Microsoft Outlook will briefly launch and close twice, taking about a minute to complete.

Following implementation, users can go to "Tools: Address Book: Show names from the:" to see the additional directories listed in their Windows Address Book.

The Navy Marine Corps Intranet (NMCI) is DON's shore-based enterprise network in the United States and Okinawa, Japan, and is part of the program portfolio of the Navy Program Executive Office for Enterprise Information Systems. NMCI provides a single, integrated IT environment for reliable, stable information transfer. ❧

Fleet Synthetic Training becomes Integral to Fleet

By LT Michael Widmann, NAS Oceana, Dam Neck Annex

VIRGINIA BEACH, VA -- Tactical Training Group, Atlantic (TACTRAGRULANT), located at Naval Air Station Oceana, Dam Neck Annex, provides the fleet with several courses and services designed to prepare strike groups, their staffs and warfare commanders to deploy successfully.

One critical service TACTRAGRULANT provides is Fleet Synthetic Training (FST). FST allows units to remain pierside and receive realistic training on their gear, in their own command and control spaces. It builds working relationships and tactical expertise in a joint environment.

The program begins with a unit level training phase (FST-U) and culminates with an FST Joint (FST-J) phase. Each phase of FST provides training in all warfare areas allowing units to maintain proficiency and master skills prior to deployment. It also allows the strike groups to correct connectivity issues before leaving the pier.

TACTRAGRULANT coordinates this training with Distributed Training Center (DTC), also located at Dam Neck. DTC provides distributed training capability to all units, including coalition and joint partners via the Navy Continuous Training

Environment (NCTE) network.

Computer simulation allows warfighters to reinforce tactical principles and doctrine in a safe environment. The TACTRAGRULANT staff can design specific circumstances to provide realistic training scenarios required by strike groups. It allows warfighters to test the capabilities and limitations of their equipment.

"Coming out of Composite Training Unit Exercise (COMPTUEX), strike groups are certified for Major Combat Operations (MCO) surge," said RADM Garry White, commander, Strike Force Training Atlantic. "The MCO surge certification is the Navy's validation of a strike group's ability to fight in an MCO scenario. The follow-on Fleet Synthetic Training-Joint or FST-J assesses the strike group staff's ability to direct and lead major combat operations, resulting in the major combat operations ready certification."

White said synthetic training has clear advantages when testing staffs because such training can incorporate joint forces, coalition partners and tactical challenges that are impractical or impossible to create amid live training at sea.

"The innovative use of modern

technology through synthetic training allows us to present more varied, realistic scenarios, and employ greater numbers of joint, coalition and opposition participants," said White. "We can simulate far more robust hostile forces and better control the conditions that a strike group may encounter during deployment. The combination of synthetic and live training more effectively and efficiently trains strike groups for combat operations and is a vast improvement over the Navy's totally live training of just a few years ago."

The Eisenhower Carrier Strike Group completed the training provided in February. FST provides strike groups the opportunity to work through planning, briefing and execution of an exercise. The simulations test various combinations of warfare areas and levels of complexity allowing leaders to truly evaluate their Sailors under stressful situations.

At the end of the simulation, strike groups are assessed and feedback is provided. FST also allows the fleet to maintain readiness within allocated steaming days and flying hours, saving the Navy millions of dollars per exercise. ❧

LETTERS FROM THE GROUND

Greetings from Baghdad!

After almost two months of in-processing, training, and travel, I've finally arrived in Iraq. One of the things I discovered along the way is that many of my fellow Navy individual augmentees had not received any information from their sponsors on how to prepare for the training or the deployment. I was fortunate enough to benefit from the advice of my sponsor, LCDR Colby McAlexander, as well as others who had previously deployed to Iraq and Afghanistan.

It's time to pay it forward!

Everything starts with in-processing at a Navy Mobilization Processing Site (NMPS). Before arriving, you may want to begin practicing something that will prove extremely important throughout the rest of your IA experience... PATIENCE. Although this is not boot camp, the experience is similar because you are going through a series of activities with a large group of people. This often results in "white space" as you are waiting for your turn. Come prepared by bringing an old-fashioned paperback book or the 21st century Kindle

(a software and hardware platform for reading electronic books); they both work very nicely.

At NMPS Norfolk, uniform fitting occurred on the first day. I'm going to tell you something that most of us don't figure out until after we leave NMPS... the fire retardant uniforms SHRINK. Don't laugh! I know it's

not the result of too much eating and not enough exercising for at least two reasons. First, I am exercising. Second, the non-fire retardant uniforms are still loose. I'm not going to make a recommendation on how you should handle the situation, but it's definitely something worth knowing about ahead of time.

There is another useful bit of information concerning the Army Combat Uniform (ACU). Before you take the uniforms out of the packaging, you may want to note which pieces are fire retardant. It is important to keep the fire retardant blouses and trousers together. You don't want to mix a fire retardant blouse with non-fire retardant trousers or vice versa for obvious reasons. You also don't want to mix them because the materials are different colors, which isn't noticeable until you are outside in the sunlight.

Getting boots that fit properly is critical. You are going to spend a lot of time on your feet, both in training and in theater. There are multiple brands of boots (Altama, Bates, Belleville, Danner, etc.) and each one has a different fit. Ladies, you will be trying on men's boots. For most of you it will not be a problem; for those with small feet, it will be. If you have time, try to figure out what brand and size fits best ahead of time. The fitting room does not carry the less frequently used sizes and it can be tough to guess what size will work for you.

Welcome to the Narmy! Once you arrive at your Army training station, you start to appreciate what our Army brethren do on a daily basis. We often hear that training is tougher than the deployment, and it's true for most of us. You should show up in relatively good shape because it is physically demanding to wear the Interceptor Body Armor (IBA) while you are firing weapons, marching, clearing buildings, etc. There is a significant caveat. If you feel almost all of the weight of the IBA on your shoulders, it is not fitted properly. Most of the IBA weight is supposed to be carried by your torso. Ask your drill sergeants for assistance. Training might be uncomfortable, but it is not supposed to be painful!

I can't talk about the IBA without mentioning its constant companion, the Kevlar helmet. Again, the fit is extremely important. What most of us don't realize immediately is that the IBA and helmet can fit just fine as long as we are upright, but turn into a tremendous pain in the neck (literally) in the prone position.

I found out about this next tip after I experienced the most profound frustration I've felt in quite some time. Before you try to fire in the prone position with IBA and helmet, unsnap your throat guard to give yourself an additional inch or so of movement. Ladies, you may have an additional complication. I went into training with long hair in a French braid and discovered that the extra bulk made it extremely difficult to fit the helmet and position myself in the prone position. I chose to cut my hair; others let their hair down while firing and put it back up when they were finished. Before you make your choice, remember that the hairstylists/barbers in theater have very basic skills.

The good news is that the drill sergeants are there to help, and they do not treat you like a boot camp recruit.

If you approach Narmy training with a good attitude and sense of teamwork, everyone will benefit. Have a great Navy day! ✂

Susan BryerJoyner

EDITOR'S NOTE: CDR BryerJoyner is currently assigned as the Chief, Knowledge Management Branch, Multi-National Force – Iraq, Baghdad, Iraq. She was previously the flag aide at NETWARCOM and Chief Staff Officer on COMCARGRU 8 staff.

Official U.S. Navy Photo



CDR Susan BryerJoyner

IT1 raises Bar for Excellence at NCTS San Diego

From NCTS NMCI Det. San Diego

Being the “first” in any situation not only sets an individual apart from the rest of his or her peers, but it makes their accomplishment noteworthy. Some call such an achievement “raising the bar,” but for IT1(SW/SCW) Richard Patrick, the completion of 12 certifications during his tour at Navy Computer and Telecommunications Station (NCTS) Navy Marine Corps Intranet (NMCI) Military Detachment (MILDET), San Diego is indeed a first and one that made him his command's 2008 Senior Sailor of the Year.

Not only did Patrick complete 12 certifications, but one of them involved a rigorous 6-hour examination making him a Certified Information Systems Security Professional (CISSP) -- a credential that's usually held by a chief.

As a MILDET Technician, Patrick resolved 175 complex trouble tickets, demonstrating his ability to handle complex issues while providing mentorship to junior Sailors. He continually pursued challenging assignments and increased responsibility.

Patrick became the first Sailor in the CNO's Special Sea/Shore Rotation/Internship program, from both San Diego and Norfolk, VA, to certify as a Cisco Certified Design Associate, Microsoft Certified Technology Specialist (MCTS) Windows Vista, Cisco Certified Network Administrator and CompTIA Security+ 2008 Bridge. He went on to earn his Microsoft Certified Technology Specialist (MCTS) Windows 2008, which is a follow on for the Windows Vista certification. While accomplishing these significant advanced commercial IT certifications, he also earned his Associate of Arts Degree in Computer Studies from Excelsior College.

As the command's Network

Operations Center LPO, he guided, managed and mentored 37 Sailors who collectively earned 52 commercial IT certifications, completed 29 college courses, 412 Navy e-Learning courses, 146 individual Job Qualification Requirements and expertly resolved more than 4,000 documented trouble tickets while providing intermediate and advanced level troubleshooting to the 500,000 end users on one of the world's largest networks.

According to LT Henry A. Martinez II, the detachment's officer in charge, Patrick's positive approach and quest for process improvement were key ingredients to making the NCTS NMCI MILDET, San Diego, the model for future public-private information technology initiatives.

“Petty Officer Patrick is an innovator in every sense of the word!” Martinez said. “He single-handedly evolved the program's Third Year Program from concept to an implemented position.”

Through the 3YP concept, Patrick spent countless off duty hours designing, developing and implementing a new course curriculum for CompTIA Security+ certification training classes, in support of the DoD Instruction 8570.1M, to provide CompTIA Security+ training to Sailors from other commands.

Two years ahead of schedule, he earned his CompTIA Network+, Security+ and Microsoft Certified System Administrator Windows 2000 commercial Information Technology (IT) certifications.

CompTIA Security+ validates knowledge of systems security, network infrastructure, access control, assessments and audits, cryptography and organizational security. It is an international, vendor-neutral security certification that is taught at colleges, universities and commercial training centers

Official U.S. Navy Photo



IT1(SW/SCW) Richard Patrick

around the world.

Patrick was personally responsible for the Security+ classroom instruction of 76 Information Systems Technicians from local shore and afloat commands. Additionally, he and IT2(SW/AW) Eric Sebring were the program's first MILDET Sailors to travel to other commands to provide CompTIA Security+ training within NMCI Det San Diego's area.

Together they provided this training to 11 Sailors from NAVCOMTELSTA Communications Unit Oklahoma City. Since his departure, the Certified Technical Training Team has continued to push forward, using the curriculum he developed to teach an additional 142 Sailors and government employees from 26 different commands.

Patrick's training initiative has already saved the Navy an estimated \$261,600 in outsourced vendor costs. Classes continue to fill up months in advance and as a result of this tremendous effort in support of the fleet. ✂



40th Anniversary Ceremonies honor 30 Fallen Sailors & One Marine

NIOC MISAWA

By MC2 Travis K. Burcham

A memorial ceremony at NIOC Misawa, Japan, recently honored the 40th anniversary of Deepsea 21's fallen crew. On April 15, 1969, 30 Sailors and one Marine lost their lives when two North Korean fighters shot down their unarmed Navy EC-121 aircraft from Fleet Air Reconnaissance Squadron ONE based at Naval Air Facility (NAF) Atsugi, Japan.

CTI1(AW/NAC) Eli Redstone, who organized the event with SN Grant Dempsey, spoke of why he volunteered to organize this year's ceremony.

"This is a ceremony we put on annually to honor individuals who worked under similar conditions that many Sailors still do today," said Redstone.

"The crew of the EC-121 paid the ultimate price in defense of these ideals. Honoring the legacy of those who had to go through such a horrific event is the least we can do."

"We want to make sure these guys aren't forgotten," Dempsey said.

Many details of the unprovoked attack are not known, including exactly how the large aircraft disappeared from the radar screen after being engaged by North Korean MiGs.

The known facts are these: at 7 a.m.

that April morning, the crew took flight from NAF Atsugi heading for the Sea of Japan. Roughly six hours into the routine mission, word came of the presence of North Korean fighters in the area. Once the impending interception of the fighters had been identified, the decision was made to abort the mission and return home.

Unfortunately the slow, propeller-driven EC-121 was unsuccessful in avoiding the much faster fighters. At 1:47 p.m. local time, the radar screen displayed the fighters meeting the EC-121. The Navy aircraft disappeared and was never heard from again.

"This memorial service is held as close to the ocean as possible in recognition of the sea as a fitting resting place for Sailors who have given their lives in service to their country," said CAPT James Haugen, NIOC Misawa's commanding officer.

Due to national security issues and secrecy surrounding the mission, little was released to the media and the incident quickly faded from the headlines. The memorial ceremony is a way to remember these Sailors and Marine who made the ultimate sacrifice.

Haugen added, "Indeed, the many unanswered questions surrounding the shoot down of Deepsea 21 will



(Right) CTI1(AW/NAC) Eli Redstone rings the bell twice at the reading of the names of servicemembers killed when their EC-121 was shot down in 1969. (Official U.S. Navy Photo)

in all probability remain a mystery, as none of the crew survived, the aircraft went down in waters too deep to recover and the perpetrators of this heinous act have not shared the truth of what they know."

Redstone reflected on the event. "I was proud to see so many dedicated Sailors come together to honor our fallen Shipmates. The event was very somber, respectful and moving. At no other time in my naval career have I felt as honored to be part of such a historical legacy as both a Sailor and air crewmen." ✍

NIOC HAWAII

By CTI1(AW/NAC) Jennifer Schooley, NIOC Hawaii

A memorial ceremony at Naval Information Operations Command (NIOC) Hawaii honored the 31 lives lost when their reconnaissance plane, an EC-121, was shot down by North Korean fighters 40 years ago. The ceremony was organized by CTI1(AW/NAC) Richard Linsley.

The EC-121 crew included 30 Navy men and one enlisted Marine. They were flying a routine reconnaissance flight in accordance with all international laws at the time of the attack. The crew was given orders to approach no closer than 50 nautical miles off the North Korean landmass, and it was actually 90 miles away from the North Korean landmass when it was heard from last. This unarmed aircraft with no combat mission and no way to defend itself, was shot out of the sky, taking the lives of every crew member. Out of the 31 souls on board, only two bodies were recovered and returned to their families.

This year marks the first year for a ceremony at NIOC Hawaii. Linsley has participated in this ceremony for nine years at other commands, and decided this year to take it upon himself to bring this ceremony to his new command. He felt the tradition of this ceremony not only honors those who have sacrificed everything for their country, but also serves as a way to remind Sailors today of how important they are to the mission. He said, "It is important we, as an aircrew community, maintain our traditions because too often we find when we don't we lose a sense of purpose and a sense of vision. By looking back at the sacrifices of our predecessors, we'll maintain our purpose and vision."

Next year Linsley hopes to see the ceremony welcome air crewmen from all over the island in an effort to remind



(Right) CTI1(AW/NAC) Richard Linsley delivers a speech during NIOC Hawaii's first memorial ceremony remembering those killed by North Korean MiGs 40 years ago. (Photo by IT3 Jai Pellerin)

everyone of the important role in remembering the past.

CTICM(SS/NAC) Ronald Stevenson, NIOC Hawaii N3's leading chief petty officer, also emphasized why this ceremony was so important.

"From the perspective of the EC-121 shoot down by the North Koreans, we have to remain vigilant," Stevenson said. "When looking back at these tragic events and seeing today, 40 years later, North Korea is still an area we have to watch closely; remembering these incidents only furthers our mission and encourages our Sailors to persevere." ✍



Performance at Sea

NAVY'S INTERNET PROTOCOL EFFORT INCREASES SATELLITE & NETWORK PERFORMANCE AT SEA

Story by Steven Davis, SPAWAR Public Affairs

Photo Illustration by MC2(SW/AW) Justin L. Ailes

SAN DIEGO - Sailors aboard the Navy's command and control ship USS Blue Ridge (LCC 19) recently received a boost in broadband connectivity thanks to the Serial Circuit Elimination (SCE) initiative being conducted by the Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I).

The initiative will increase the speed and reliability of satellite communications and computer network performance by providing Navy ships with greater throughput (the average rate of successful message delivery over a communication channel). This is attained by reallocating satellite communications bandwidth. Restructuring dedicated, but seldom-used, communications

circuits into a shared bandwidth pool managed by a network router frees up the bandwidth.

The SCE solution uses Internet Protocol (IP) transport to convert data into IP packets similar to those for computer networks. The packets are then sent through the main Automated Digital Network System (ADNS) router that dynamically assigns the bandwidth necessary to transport the packets through the satellite link.

LT Benson Lo leads the SCE team for the Space and Naval Warfare Systems Center Pacific. Lo likens the serial circuit transition to the transition from regular telephones to Internet telephones that use Voice-over-IP (VoIP) packet switching technology.

"Packet switching is a more efficient way of transporting data,"

said Lo, "and while most home users may not think about efficiency, in a resource-limited environment at sea, every little bit counts."

Traditionally, satellite voice and data circuits on Navy ships, such as phone lines and special intelligence data networks, are aligned in a serial architecture. These serial circuits are automatically assigned a dedicated portion of the available satellite bandwidth and do not share that assigned portion with other circuits when not in use. These inflexible and inefficient "stove-piped" circuits also use outdated multiplexing and encryption equipment that limits data rates and are expensive to maintain. The SCE initiative eliminates the need for serial circuits and frees up bandwidth for dynamic and efficient allocation using a network router.

Another limitation, according to Lo, is that most serial circuits connect to the satellite link via a multiplexer, called TimePlex, which has a switching rate limitation of 2 Mbps.

"The rate limitation is a bottleneck in the data path, and it poses an obvious problem as our ships transition to new satellite communications terminals capable of above 20 Mbps. Converting the circuits to IP routed through ADNS bypasses the TimePlex" explained Lo.

In October 2008, Lo's team moved a serial intelligence data circuit aboard USS BLUE RIDGE (LCC19) into ADNS and freed up more than 10 percent of the ship's bottlenecked bandwidth. LTJG Jerry Woods, BLUE RIDGE radio officer, is pleased with the change.

"The Navy's move to an IP-based infrastructure is definitely a step in the right direction," said Woods. "The [intelligence] circuits are working much better over IP and we are able to better use our available bandwidth allocations."

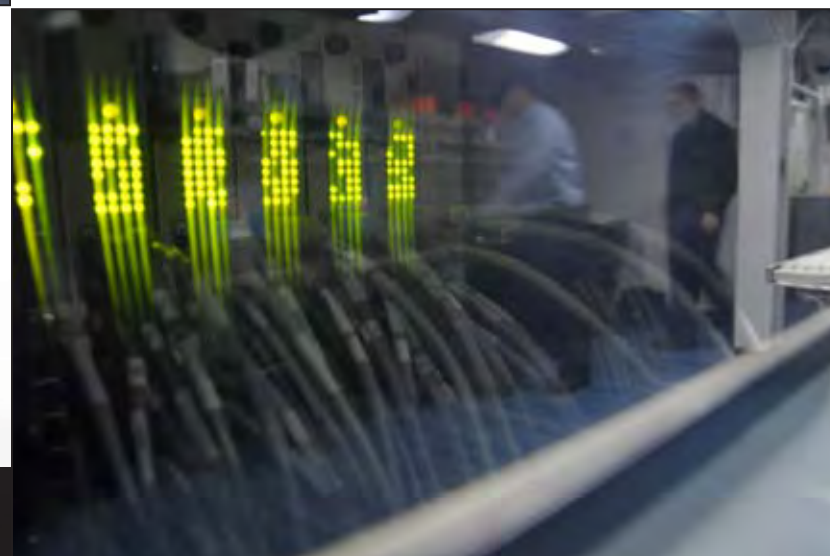
According to Lo, not all Navy circuits will be as easy to transition. Some of the circuits will require a major architecture change at the shore termination point -- a change that will involve non-Navy agencies. Lo's team has already begun coordinating with the Army and NATO to convert some of the circuits.

Lo believes that when the SCE is completed, Navy ships will carry a modern, all-IP communications architecture that includes IP video teleconferencing and VoIP. ✕



(LEFT) SPAWAR government employee Fran White (left) and Tactical Networks Program Office (PMW 160) contractor Clayton Bush work with Navy Information Systems Technician 2nd Class James Rago while troubleshooting systems in the Strike Group war room on board USS Ronald Reagan (CVN 76). SPAWAR and PMW 160 provide the Navy with network fabric and services used by multiple shipboard tactical and business applications and systems and routinely install, maintain and train crewmembers in operational and maintenance procedures. (Photo by Rick Naystatt)

(RIGHT) Lights flash to indicate server activity in the unclassified Automated Data Processing (ADP) workspaces on board USS Ronald Reagan (CVN 76). The Navy's Tactical Networks Program Office is responsible for afloat networks and is overseeing the CANES system development initiative. (Photo by Rick Naystatt)



KEY POINTS

NAVY SHIPS CURRENTLY USE SERIAL CIRCUIT ARCHITECTURE, WHICH LIMIT DATA RATES AND ARE EXPENSIVE TO MAINTAIN.

NEW PEO C4I SOLUTION USES INTERNET PROTOCOL TRANSPORT TO CONVERT DATA INTO IP PACKETS.

SOLUTION FREES BANDWIDTH FOR DYNAMIC, EFFICIENT ALLOCATION USING AN AUTOMATED DIGITAL NETWORK SYSTEM ROUTER.

SOLUTION INSTALLED OCTOBER 2008 ABOARD USS BLUE RIDGE (LCC 19) FREED UP MORE THAN 10 PERCENT OF THE SHIP'S BOTTLENECKED BANDWIDTH.



NCDOC COMMANDER NAMED TO 2009 FEDERAL 100 LIST

By MC2 Adrian T. White

CAPT Roy S. Petty, commanding officer, Navy Cyber Defense Operations Command (NCDOC), at Naval Amphibious Base Little Creek, has been named to the 2009 Federal 100 list of outstanding leaders in the federal information technology (IT) community, and was recognized recently at the Ritz-Carlton Hotel in McLean, VA.

Petty received the honor from Federal Computer Week (FCW) magazine for leading the effort to strengthen the defenses of Navy networks and coordinating similar efforts across the Global Information Grid.

FCW initiated the Federal 100 list 20 years ago, to recognize individuals from government, industry and academia who significantly influence how the federal government buys, uses or manages information technology (IT). Honorees are nominated by FCW readers and evaluated by an independent panel of judges for their risk-taking, vision and pioneering spirit.

Petty credited the award to the hard work and dedication of the NCDOC team in bringing the cyber fight to the enemy.

"I've had the great fortune to be in command of a truly outstanding organization at a time when the Department of Defense and the nation are extremely focused on the issue of network security and defending the critical infrastructure," Petty said. "What I am proudest of is the tremendous capability improvements we've brought to the fight; the building of real knowledge, processes, and capabilities."

Under Petty's leadership, NCDOC became the first Computer Network Defense Service Provider in the Defense Department to receive a Level 3 accreditation from the U.S. Strategic Command.

"The Computer Network Defense mission is essential to every other warfare area and requires commanders at every level understand it's importance," Petty said. "The Navy's networks are absolutely vital to our war-fighting capability and they are a vulnerability that must be protected."

Petty has also been selected as one of the Department of the Navy Chief Information Officer (DON CIO) Information Management/Information Technology Excellence Award winners for his excellence in leadership and efficiency as it relates to the DON IM/IT strategic vision.

"Captain Petty leads from the front and maintains a vision for his command that far exceeds the daily expectation of a commanding officer," said DON CIO Robert Carey.

Petty said that while NCDOC and the military have accomplished much in the cyber arena, there is still much left to be done.

"I believe the most significant accomplishment we've achieved is bringing the fight to the forefront," he said. "Our environment demands that we find more creative ways to leverage the power of a networked culture to share information and collaborate seamlessly in a real or virtual global environment. However, this must be balanced against an increasingly agile threat that adapts far quicker than our traditional ability to respond."

"Additionally, we cannot expect technology to solve our problems," he said. "The challenges we face require a combination of people, operations, and technology. And we can never be satisfied; there will always be more to do." ✂



NCDOC Commanding Officer, CAPT Roy S. Petty observes IT3 Thomas Sikes as he conducts his daily watchstanding duties. (Photo by MC2(SW/AW) Justin L. Ailes)

NETWORK SECURITY 101

Story & Graphic Illustration by MC2 Travis K. Burcham

The emergence of cyberspace as a national security frontier has thrust network security to a place of preeminent importance within the Department of Defense. It's accurate to state that as long as computers are used to access networks, DoD systems will be vulnerable to security breaches. The threat this poses to critical information systems – and the data contained on them – are as real and significant as physical threats. The Navy employs a dedicated team of experts across the globe, working to preserve the unhindered and uninterrupted operation of Navy computer networks.

Lessons learned from past network breaches and the recent DoD prohibition on the use of thumb drives underscore the intensity of the current focus on network security. And, while this is a full-time mission for Navy Information Systems Technicians (ITs), Information Assurance Managers (IAMs) and other cyber warriors, the reality is that the security of our networks rests on the shoulders of every user. The E-1 checking his unclassified email has as important a role to play in keeping Navy information technology (IT) resources secure as the senior officer or civilian manager accessing the Internet.

In a message to Navy leaders in 2008, Chief of Naval Operations, ADM Gary Roughead reaffirmed that protecting our networks begins with each user, as well as commanders who are actively engaged. "Threats we face demand that we be meticulous and vigilant," Roughead said. "Our networks are critical operational systems that require (commanders') personal visibility and involvement."

The following guidance is provided by the Naval Network Warfare Command Information Assurance Management team to help users understand how to

operate safely and securely in the cyber realm. Every Sailor, Navy civilian and contract employee should keep these policies and procedures in mind when using a government computer.

DEFENSE IN DEPTH

Navy and DoD are using a layered defense strategy to protect our networks and the information carried on them. Defense in Depth requires three basic elements:

- **PEOPLE** – Written policies, training, incident response teams
- **PROCESSES** – Management oversight, commitment of resourced budget, contingency planning
- **TECHNOLOGY** – Firewalls, public key infrastructure, anti-virus protection, integrity assurances.

INFORMATION ASSURANCE TRAINING

All active duty, Reserve, civil service, contractor and/or foreign national personnel who have been granted access to or who are providing services for Navy IT resources are required to comply with the Navy's Information Assurance (IA) program. User training is a vital part of a successful Defense In Depth strategy, and the Navy has mandated annual training in IA for all users. Completion of the training requirement is tracked in Navy Knowledge Online (NKO) and by the user's command.

Consent to Monitoring

There is no right to privacy over DoD networks, and any DoD computer use is subject to monitoring. Though perhaps unnoticed by many, the DoD user agreement

banner pops up with every login. This message clearly states the monitoring policy and should be fully understood before the "OK" button is clicked.

E-Mail Access and Accounts

E-mail has turned into a primary source of communication, both classified and unclassified. Improper use of government e-mail can open a number of vulnerabilities into a system.

Some Web sites are blocked from access by DoD computers, as many of these sites have messaging capabilities such as e-mail. The use of commercial e-mail accounts on government systems is prohibited for two reasons. The first is the threat of malicious code attacks (such as a virus or Trojan), and the second major vulnerability is the possibility of classified information being inadvertently transmitted to a commercial system. Another threat would be created by forwarding messages from a government account to a commercial account. Within this scenario, the sender wouldn't know the classified information is leaving a secure system if the recipient has the account configured to send all messages to an outside e-mail server.

ACCESS CONTROLS AND SECURITY

The user is the Navy's first and best defense against security vulnerabilities. Government employees dealing with valuable information are required to log into Navy networks using access controls such as Common Access Card (CAC) and a Personal Identification Number (PIN). In a secure environment, access controls are necessary to allow network administrators to configure user accounts based on the individual's "need-to-know." Even though a security clearance may be in place,

the individual might not require knowledge of certain information to effectively perform his or her job. This means that the employee has the necessary security clearance but not a need-to-know, and the network administrator can then limit network access based on the individual's authorized access level.

The extent to which our adversaries are willing to go to gain access to Navy networks often goes unseen. But, attempts are made each day at an alarming rate, requiring reliable access procedures for authorized users.

When one logs into a government computer, access is gained to the network. If the CAC and PIN used to gain access is obtained by an unauthorized person or organization, those outside users now have that same level of access to the network and the information on it. Even if that information is unclassified, in the wrong hands that basic level of access can be used as an open door to gain further intrusion to the network.

The weakest link in network security is the person who practices poor operational security and fails to protect their CAC and PIN that allows access to the network. Common mistakes include leaving one's CAC in the reader when stepping away from the computer, or leaving a written PIN near a workstation for easy access. While convenient for the user, these practices make it immensely easier for others to gain access to the system. All DoD computer users must place a personal emphasis on protecting their CAC and PIN.

Users must also remember that some networks still require user names and passwords to gain access. Those passwords carry the same classification levels as the systems to which they allow access. For example, if the workstation being used is Secret, so is the password.

NETWORK SECURITY 101

IMPROPER USE OF INFORMATION TECHNOLOGY RESOURCES

If you think that classified information is being used inappropriately, report it to your supervisor. Vulnerabilities must first be known to be resolved.

The Designated Approving Authority (DAA) is responsible for issuing a written authorization for connectivity and operation of Navy IT resources. The use of privately-owned hardware and software is prohibited at all times and under all circumstances unless specifically authorized by the DAA or a delegated official. Running executable files increases the threat of viruses and other network vulnerabilities, including numerous types of malicious code. Only use approved hardware and software when working on a government workstation. When in doubt, seek guidance from your command IAM.

VIRUSES AND MALICIOUS CODE

Millions of dollars are spent by government and private industry to undo the damage associated with viruses and malicious code.

New viruses are found every day, which is why it's extremely important that DoD systems have the most current virus scanning software available. System administrators update the virus scanning software when new viruses are discovered.

As a user, you can ensure you don't introduce malicious code or viruses into the network by scanning all documents with an anti-virus program before you open or save them to the computer. In most cases, the anti-virus software will do this automatically, but there are exceptions. When working with removable media such as CDs or DVDs, the software may not automatically run a scan. Don't assume that the

information is clean and free of malicious code or viruses. Always check to make certain.

COMPUTER SAFETY AT HOME

All of the security measures taken at work apply to personal computers at home.

- The active protection of passwords and personal information diminishes the threat of identity theft.
- The use of virus scanning software decreases the possibility that your computer could become infected with a virus, worm, or other type of malicious code.
- Patch, patch, patch! Nearly 90% of network incidents in 2008 were avoidable through existing security patches, policy or other controls. The latest patches and upgrades for your system block numerous threats against your personal computer. Active duty military and government employees are entitled to free anti-virus and firewall programs, so take advantage of them. Check with your command's IAM or information systems technicians for more information on acquiring anti-virus software.

To learn more about network security in the Navy, visit the Department of the Navy Information Assurance Web site at <https://infosec.navy.mil>. ☞

REMEMBER *you are a very important link in this critical chain to preserve the integrity of our information networks.*

Center of Excellence, there are actually several outstanding EW "centers of excellence" that already exist in the Navy today: NAS Whidbey Island is the center of tactical and operational EW expertise, and home of the EP-3 'Aries II', the EA-6B 'Prowler' and now the EA-18G 'Growler'; Naval Surface Warfare Centers (NSWC) Crane, IN and Dahlgren, VA; Naval Air Warfare Centers (NAWC) Point Mugu, China Lake, CA and PAX River, MD are also centers for EW technology efforts; the Office of Naval Research (ONR) and Navy Research Lab (NRL), Research and Development (R&D) and Science and Technology (S&T) centers are also centers of excellence. The challenge today is to coordinate and integrate these disparate centers of subject matter expertise into a cohesive group focused on a strategic investment for Navy electronic warfare. The coordination and the integration will be the primary missions for the FEWC and the EW FCT.

What will the FEWC's primary mission be and how will it guide and support the Navy? What are its goals, limitations and future?

The FEWC's primary mission is to be the fleet's center of gravity for EW operational and tactical concerns, both material and non-material. As the organization within NETWARCOM, it will answer daily to higher echelon EW taskings, augmenting staffs without EW expertise, while simultaneously performing the administrative and managerial functions required to run the new, United States Fleet Forces - established EW FCT.

The goal of the FEWC is to constantly keep VADM Starling informed, in his role as the Navy's Operational Agent for EW, and to advise the Fleet commander on EW readiness issues. VADM Starling has built the FEWC as a small corps of cross-platform officer and enlisted EW expertise that has worked hard and developed initial credibility and legitimacy. A key to success will be to focus on accomplishing what we can with what we have now. The future scope of the organization will be determined by the demand signal from the Fleet.

What are the roles and responsibilities of the EW Fleet Collaborative Team, and what is its relationship to the FEWC?

The EW FCT will be the primary EW integration organization for Fleet concerns. As stated earlier, the EW FCT is chaired by VADM Starling who will appoint three flag officer/SES-level Integrated Process Team (IPT) directors to focus on EW manning and training, EW doctrine, and EW technology.

The Flag Officers will be supported by an Executive

Steering Committee consisting of empowered fleet members (within the USFF claimancy): U.S. Fleet Forces, U.S. Pacific Fleet, all numbered Fleets, all five TYCOMs, Naval Warfare Development Command, Strike Force Training Atlantic and Strike Force Training Pacific, Patrol Reconnaissance Group and Electronic Attack Wing Pacific. They will be assisted by consulting members from OPNAV codes N2, N3/5, N39, N6F, N86, N87, N88 and N89, Naval Special Warfare Command, Office of Naval Research, Joint EW Center, Bureau of Naval Personnel, and other organizations as needed. As a final product, the EW FCT will develop and submit an annual EW Integrated Priority List for submission by VADM Starling to the Fleet Commander. The EW IPCL will represent a consolidated view of EW priorities across the fleet for use by OPNAV to resolve EW capability gaps.

The FEWC will be the small cadre that helps to keep the life blood pumping through the EW initiatives being addressed by the EW FCT, the IPTs and their supporting teams as required. The FEWC will be the constant EW touch point which anyone in the Fleet can rely on to raise the visibility on EW issues to the EW FCT. The FEWC, located at NETWARCOM, will work EW challenges as their primary job, whereas the EW FCT will be a collaboration of geographically-dispersed EW expertise, linked together virtually to address specific EW challenges in addition to their other primary duties. In many ways, the FEWC can be likened to an engine to drive or sustain the EW FCT efforts.

Why is the chance of success for improving Fleet EW readiness any better than before?

We are in a time of unprecedented levels of visibility on the critical impacts that electronic warfare capability and capacity have on today's fight. Component Commanders have articulated their EW challenges and impressive analysis has been performed by the Joint EW Center in the form of extensive EW Capabilities and EW Functional Solutions Analyses. These efforts will be addressed at the 4-Star level in the Pentagon, and will influence service investments in EW.

There is new opportunity to work solutions through coordinated efforts and develop insightful strategic investment plans. The Fleet has answered the challenge by establishing the FEWC and the EW FCT to increase the focus on Fleet EW. NETWARCOM is now the single point of contact for Fleet EW. The FEWC will continue to work together with EW subject matter expertise across the nation and throughout the Fleet to enable the EW FCT to prepare an annual integrated, prioritized cross-platform list of challenges to the Fleet Commander. The end result will be successfully enhanced EW readiness for the Fleet. ☞

Fleet Electronic Warfare Center

CHANGING THE FACE OF COMBAT

Story by George D. Bieber

Photo Illustration by Travis K. Burcham

“Electronic warfare is essential for America to maintain its military superiority. Electronic warfare provides access to the battle space, degrades our enemy’s capability to attack, and, most importantly, saves lives.”

-Congressman Joseph R. Pitts, Chairman, Congressional EW Working Group

The demand for a focus on Electronic Warfare (EW), heard from Congress as well as from combatant commanders, is greater than ever before. The incredible pace of technology advances from near-peer adversaries, and recent military actions have highlighted EW capacity and capability challenges in support of joint commanders around the globe and have direct application to our ability to perform Navy missions. These significant developments demanded that we examine our current constructs and processes responsible for maintaining an edge in EW.

Praising Navy efforts at a recent Electromagnetic Spectrum (EMS) Control Conference in San Diego,

CAPT Brian E. Hinkley, lead for the newly established Fleet Electronic Warfare Center (FEWC) addressed NETWARCOM’s innovative focus on Fleet EW and operational control of the EMS.

“NETWARCOM has established the Fleet EW Center, the first organization of its kind in my 26 years of active service that the Navy specifically created with an unbiased focus on EW across all platforms,” said Hinkley. “We’re looking at EW throughout all warfighting domains, as a holistic warfare capability, instead of addressing EW capability by individual platforms that historically compete against each other for limited resources. Additionally, with Operational Control (OPCON)

of the Navy Marine Corps Spectrum Center, the FEWC has been able to realign fleet spectrum expertise to be more responsive to spectrum control requirements from each of the Numbered Fleets across the globe.”

Fleet and industry representation at the conference agreed the Navy’s ability to control the increasingly congested and contested electromagnetic spectrum at the time and place of our choosing will determine our ability to influence and defeat future adversaries.

“The Navy cannot presume unimpeded use of the spectrum,” added Hinkley, “therefore, it is proactively focusing on EW material and non-material challenges at new, higher levels.”

NETWARCOM, as the Navy’s



138-144 MHz

LAND MOBILE RADIO
TACTICAL AIR/ GROUND/AIR

225-400 MHz

TACTICAL AIR/ GROUND/AIR
DATA LINKS
SATELLITE COMM
MILITARY ATC
SEARCH AND RESCUE
EXECUTIVE COMM
TACTICAL COMM

400.15-401 MHz

OMSP

420-450 MHz

BM SURVEILLANCE AND EARLY
WARNING RADARS
SHIPBOARD/AIRBORNE EARLY
WARNING RADARS
MISSILE/AIR VEHICLE FLIGHT
TERMINATION
TROOP POSITION LOCATION
ANTI-STEALTH RADAR
FOLIAGE PENETRATION RADAR

1215-1390 MHz

LONG/MEDIUM RANGE AIR DEFENSE
RADIO NAVIGATION
AIR ROUTE SURVEILLANCE RADARS
TACTICAL COMMUNICATIONS
TEST RANGE SUPPORT
AIR/FLEET DEFENSE
DRUG INTERDICTION
GPS
REMOTE SATELLITE SENSORS
NUCLEAR DETECTION

1435-1525 MHz

TELEMETRY SUPPORTING ENTIRE
AEROSPACE INDUSTRY

1755-1850 MHz

ODD SATELLITE TT&C
POINT-TO-POINT MICROWAVE
AIR COMBAT TRAINING SYSTEMS
TACTICAL COMM
TACTICAL DATA LINKS

2200-2290 MHz

ODD SATELLITE TT&C
GUIDED MISSILE TELEMETRY
POINT-TO-POINT MICROWAVE

3100-3650 MHz

HIGH POWER MOBILE RADARS
SHIPBOARD ATC
MISSILE LINKS
AIRBORNE STATION KEEPING

4400-4940 MHz

FIXED WIDEBAND COMM
MOBILE WIDEBAND COMM
COMMAND LINKS
DATA LINKS

“The Navy cannot presume unimpeded use of the spectrum ...”

Operational Agent (OA) for EW, recognized the need for this focus, and recently created the FEWC to be the Fleet’s center of gravity for EW issues and concerns. VADM H. Denby Starling II, Commander, NETWARCOM, working together with the other TYCOMs, will address deficiencies in EW manning, training and equipping that impact Fleet EW readiness, and advise the Fleet Commander on critical EW challenges.

The FEWC has built its initial credibility swiftly. It consists of a small group of EW professionals with backgrounds from all warfighting domains. Officers from naval aviation electronic attack (VAQ) and electronic warfare support (VQ) communities, senior enlisted from the surface warfare community and government service employees with decades of spectrum management experience. Additionally, a wealth of expertise and experience comes from civilian contractor augmentation, most with extensive former military EW backgrounds.

Unimpeded use of the EMS and robust EW capability is crucial to joint operations now and will continue to be in the future. NETWARCOM has taken on the challenge to advise the Fleet Commander on Fleet EW readiness across the range of doctrine, organization, training, material, leadership and education, personnel and facilities (DOTMLPF). The command is poised to recommend potential solutions to future EW challenges by coordinating EW and spectrum expertise across the nation.

“Congressman Pitts stated that EW is essential to maintaining military superiority. With its new focus,” said Hinkley, “NETWARCOM is essential to Fleet EW.”



(Center) CAPT Brian Hinkley, FEWC lead, discusses new items from a recent conference with EW staff members. (Photo by MC2 Adrian T. White)

NETWORK & OPSEC BLUNDERS

From NIOC Norfolk

Welcome to the first edition of the Navy Network and OPSEC blunders as seen through the eyes of your Navy Blue Team, Red Team, and OPSEC Support Team.

These three teams, hosted at Navy Information Operations Command Norfolk, were established to improve fleet network and operations security through training and readiness assessment. Part of that mission is to conduct cooperative and non-cooperative assessments of units, strike groups, and shore commands to help commanders assess their actual security posture. Keep in mind as you read through these “blunders” that they are all preventable.

If commands are following standard network and operations security procedures, most of the things you read below would simply not happen.

A. First, a thank-you from the “bad guys” to everyone who keeps wearing their badges off base. Not deterred by all of those warnings from your security team, you proudly display your importance to national security at the NEX, mini-mart, hotel lobby, casino, etc. While yes, you look important, you are helping us to gain access to your work spaces.

It is very easy to get a picture of your command or community badges, make a copy, and sit down next to you in your building, ship, or “secure” facility. Once we’re in and able to move around at will it’s simple to “shoulder surf” through your emails, drop in on your conversations, and possibly use the computers in your building to get about everything we need to know. Here’s to you off-base badge wearer!!

B. Do you recall having training on challenge and response? Here’s a summary -- if something or someone appears to be out-of-place, challenge that person for ID, or at least bring your observations to your chain of command or security officer.

For example, we recently sent two folks into a secure facility by piggybacking on a command member. The individuals attempted to gain entry to an inner (more secure) room, but a senior military member stopped to challenge them. Good for him, but their made-up story about “doing security checks” worked and he released them without making them show credentials!

C. Who doesn’t love forwarding email from people they have never met?! Unfortunately, no one informed a command master chief on a surface ship what to do with a potential phishing email. He sent it to 1... 2 ... no 6 other chiefs, and the ship’s captain. All opened the email, and all compromised their computers, allowing future Red Team exploitation.

While this time it was just us, your Red Team, sending the email for training purposes, it could have been a real-world adversary, with real-world information/system/

network compromise. If you receive an email from someone you do not know, be careful and question it. If you receive an email from someone you know which looks suspicious, question it. Do not click on links or forward suspicious emails. Report the email via SPAM reporting instructions.

D. We really enjoy seeing what you’re bidding for on eBay, but should you really be using Navy assets to conduct personal purchases? ...and by the way, that second chance auction win may not be who you think it is! Besides violating Navy regulations, open areas such as eBay can introduce openings in your network security which can and will be exploited in the real world of cyber-terrorism and cyber-espionage.

E. Ever heard “loose lips sink ships?” It’s not just a clever old phrase. Navy personnel regularly give us the information we need to obtain access to your spaces, or tell us where to look for the information. The usual suspect areas are the smoke pits or lunch-time snack bar and some of these conversations are secret and above! It’s not that hard for anyone who frequents local bars or parties to imagine what might be said when alcohol is added to the mix. One such story involves a Sailor who was asked if he was in for a short time. The best answer is not, “yea, we’re just here today and flying out tomorrow.” You’re not likely to impress him/her with what you do or know from work, unless they are a foreign intelligence agent.

OPSEC violations can provide a wealth of knowledge to an adversary, including how to access and compromise our networks. Remember, “Sailors taking care of Sailors on liberty” also applies to Sailors spilling sensitive and classified information.

F. Systems administrators, your passwords procedures set the example right? Placing all of your passwords in a word document and saving it is not wise. The Red Team and our adversaries think that’s a great idea! Placing cool little pop-ups with the password on it is not recommended either. The bad guys really love that! We know you have many passwords to remember, but using the same passwords on multiple accounts is a very dangerous practice, particularly when you use the same one on an account with administrator privileges and your user account!

G. So a shop wanted to help out some friends. Who would know if they had just installed a little router in their shop...on the network to create a little subnet. Hardly noticeable at all really unless you’re a flag officer in another command and you can’t seem to get your computer to work properly anymore. This is exactly the

... continued on Page 33

NAVY RESERVE

HONOR COURAGE COMMITMENT

Naval NETWAR FORCEnet Enterprise Reserve Integration

From CAPT Michael Wilkins, NNWG Public Affairs
& Jeff Smith, SPAWARSCOM Reserve Program Office

Key members of the Naval NETWAR FORCEnet Enterprise (NNFE) total force Executive Steering Group (ESG) leadership team met to brief NETWARCOM leadership on the status of the total force integration of the NNFE Reserve Component (RC).

Led by Active Command (AC) and RC flag officers, five domain leaders (O-6's) from Signals Intelligence (SIGINT), Information Operations (IO), Network Operations (NETOPS), Space and C4 Intelligence Surveillance and Reconnaissance (C4ISR), and civilian managers, the group has made great strides since its initial charter in November 2007.

WORKING GROUP STATUS

From the original charter, which focused on evaluating how the RC best fits into the NNFE, the ESG formed six core working groups to ensure that the RC aligns to the three NNFE prioritized mission areas:

- ✓ Contingency Response
- ✓ Current Readiness
- ✓ Future Readiness

The six working groups cover: Developing RC mission employment and processes, metrics/reporting, cross program resource sharing, strategic communications, and developing contingency response plans.

Though the working groups are under various stages of maturity, a very clear picture of the strength of our RC is beginning to develop. For

example, the mission employment working group conducted a full NNFE RC capability assessment (paralleling the recent CNO Reserve Capability Review) to answer questions such as: Where are the RC personnel employed? What AC mission gaps exist? And how do we develop a vetting process for resourcing the RC to the three prioritized missions?

The NNFE Reserve force is comprised of more than 1,500 Reservists in 60 Reserve commands who possess a wide range of civilian technical, managerial, and Information Technology (IT) backgrounds, as well as an extensive set of military skills. These Reservists represent 16 critical competencies and support NNFE in areas such as: SIGINT, Intelligence/Linguistics, Satellite C2, NETOPS, Cyber Asset Reduction and Security (CARS), and Network Defense and Space.

Through meetings with the AC, several key mission areas were identified as critical future needs that the Reserves can directly support, such as: Submarine Computer Network Defense support, Fleet-based C4I Readiness, Space acquisition support, CARS, Strategic/Operational focused IP planning, and Blue/Red OPSEC support.

The working group also shared with the admirals several examples of the NNFE RC strengths. In the area of C4I Fleet support, Reserves participate in Computer Network Defense In Depth (CNDID's) missions on the networks of more

than 50 percent of all strike group deploying surface platforms. Reservists also provided more than 2,500 hours per year training Fleet students in highly technical IT subjects while embarked on nine deployments per year at a cost savings of more than \$675,000 per year.

In the Navy Computer and Telecommunications Area Master Station (NCTAMS) arena, 210 Reservists contributed more than 4,000 hours (over 1.5 years) supporting the ONE-NET installations effort in five major overseas naval installations: Bahrain, Naples, Souda Bay, Rota and Sigonella; while the RC in the IO domain is key in the implementation of Information Assurance (IA) into strike groups and joint and Fleet exercises.

The RC Space Cadre's Knowledge, Skills and Abilities (KSA) are unique in that the majority of their expertise is earned outside of the Department of the Navy.

INNOVATIONS

Some innovative initiatives are evolving out of the ESG. One is an experimental concept for naval Reserve and NETWARCOM N4 staff scrubbing critical readiness degraders of all NNFE commands who report in Defense Readiness Reporting System-Navy (DRRS-N) on a monthly basis. Reserves will put the call out to all five domains to find the reservists who possesses the correct KSA to assist those commands with the objective of improving readiness.



Photo Illustration by MC2(SW/AW) Justin L. Ailes



The reserve team is modifying the COMNAVRESFOR's Civilian Skills Matrix (CSM) database and placing it on NETWARCOM's NEWS web site. The database will provide access to NNFE reserve civilian skills. Additionally, there is a statement of work feature called the "virtual job bar" to request reserves with specific KSA to provide support for just about any requirement. The initial offering will include reservists in the C4I, NETOPS and Space domains. Look for the link in NEWS in July.

THE WAY FORWARD

The ESG and working groups have created a robust metrics and measurement CONOPS and are gathering data on capabilities delivered, operational effects and reserve readiness for tasking and mobilization. This data will help the NNFE leadership align the Reserve Force to the mission priorities and critical requirements.

VADM Starling noted that his interests for the NNFE RC are focused on "IT-specific/cyber disaster support" within the NETWARCOM scope of immediate interest. Working

group No. 6 has been chartered to move forward in the area of Contingency Response planning. To do this, the RC must become aligned with NETWARCOM N3, COCOM and CFFC planners. The reserves are key contributors to the decision superiority process, and as RADM Deets previously indicated, "We no longer have days to decide—we have minutes." Using the reserve resources effectively will exponentially improve contingency responsiveness. ✎

- Assist in determining the desired end state conditions for each relevant public and actor in terms of perceptions, attitudes, beliefs and behavior
- Assist with the campaign design, ensuring planned deeds, words and images are mutually reinforcing and likely to produce the intended change in behavior
- Assist in developing a campaign or mission narrative
- Coordinate the information engagement activities and ensure the proper integration of those activities into base plans and orders

The FA 30's assist the commander in incorporating the information dimension of their operational environment into their vision so that they effectively describe, direct, assess and leads their unit to mission success. Graduates of the FA 30 course are well grounded in the art and science of the military profession and possess a thorough understanding of full spectrum operations, IO theory, doctrine and tactics, techniques and procedures.

IO officers understand the information dimension of the operational environment, including the cultural factors that impact operations and can apply their understanding to leverage the information dimension to achieve an operational advantage that leads to mission success. Additional IO skills include the ability to seize and maintain the initiative of the information dimension from asymmetric, learning and adaptive adversaries and threats.

Many consider IO officers to be experts at identifying, assessing and solving complex problems that may confront their unit. ✎

EDITOR'S NOTE: Navy Net-Centric Warfare Group has approximately 1,500 Navy reservists from 60 Reserve commands in five domains: C4I, IO, Space, Networks and SIGINT.



(Left to Right) CDR Dean Wence – NR NIOC Washington DC, LCDR Don Savage – NSA/CSS Hawaii, LT Dan Krowe – NR NIOC Washington DC, LCDR David Salak – NIOC Denver, LCDR Thomas Ramar – NR NIOC Denver, LT Vincent Quatrone – ONI-1201, LT Michael Crino – ONI-1201. (Official U.S. Navy Photo)

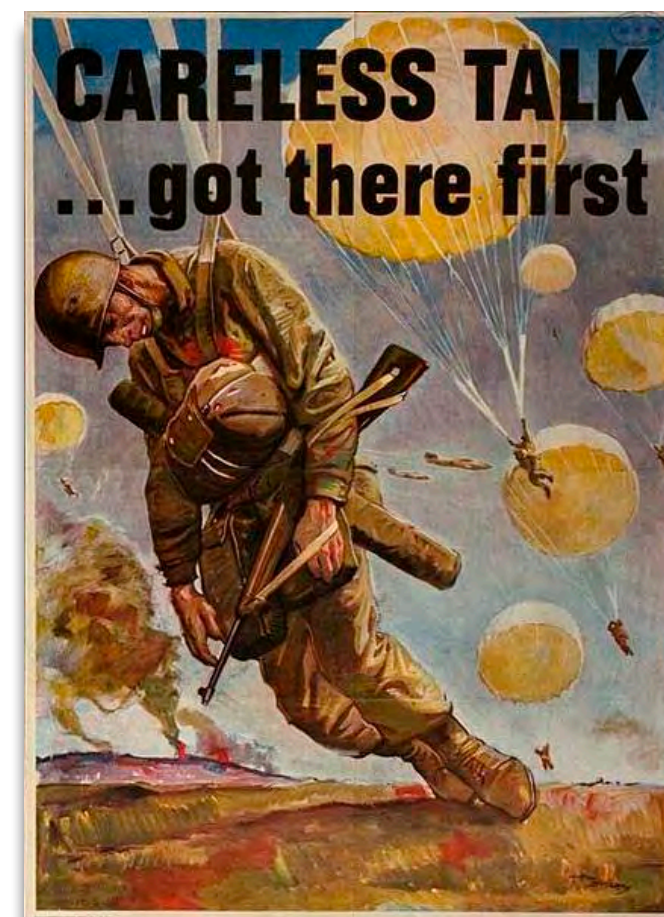
kind of equipment the Red Team can use to exploit an entire network.

As mentioned at the top of this message, simple procedures, when followed (like only using authorized equipment), have a big impact on overall network security.

H. Finally, let's revisit paragraph B, and the idea of verifying security credentials. One Red Team member strolled into an overseas facility without any documentation -- CAC card, passport, drivers license, etc.-- and was in-processed for a joint exercise. He was issued a rifle, pistol, and TS/SCI clearance with which he infiltrated the communications facility and sat in on flag officer briefings regarding force capabilities, troop numbers and movements. Nuff said!

Bottom line, while our Blue and Red Teams, as well as OPSEC Support Team try to accurately replicate an adversary, they are bound by the rules dictated by the requesting command. True adversaries are not similarly bound, so don't assume these things can't happen, or aren't happening already outside of the exercise environment.

You never know who is listening or what their intentions are. Verify, verify, verify! Memorize, don't compromise. Prevention is preferred, detection is a must! ✎



Reservists complete Rigorous Army Qualification Course

From CAPT Michael Wilkins, NNWG Public Affairs & LCDR Tom Ramar, NR NIOC Denver

Three Navy Net-Centric Warfare Group (NNWG) – Reserve officers recently graduated from the Army FA 30 Information Operations Qualification Course, at Fort Leavenworth, KS. The members were CDR Dean Wence (Washington DC), LCDR Tom Ramar (Denver) and LT Dan Krowe, also from Washington.

The FA 30 Qualification Course is the only credentialing course for the Information Operations (IO) career field for Army officers. Its purpose is to qualify IO officers prior to assuming duties at their initial IO assignments. The course develops FA 30 (IO) officers who have the requisite competencies to serve successfully on staffs at Army brigade through corps level

headquarters, which includes a thorough understanding of other Services, Joint DOD, non-DOD, non-governmental and international agencies.

FA 30 officers serve as the commander's focal point for achieving the full potential of information, engagement, communication, and collaboration in an era of persistent conflict. Specifically, they:

- Assist in identifying, analyzing and understanding those publics and actors whose perceptions, attitudes, beliefs and behaviors affect the unit's mission

NCTAMS LANT DET BRUNSWICK

Tactical Support Communications Center prepares for Closure

By Tom Brewer,
NCTAMSLANT DET
BRUNSWICK, ME

The mission of the Naval Computer and Telecommunications Area Master Station Atlantic Detachment (NCTAMS LANT DET) Brunswick, ME, hasn't changed much over the years. The command still supports Navy P-3 aircraft in conducting maritime patrol and reconnaissance operations. It still maintains the communication link between Patrol and Reconnaissance Wing 5 (VP-5) aircrews and their Tactical Support Center (TSC). NCTAMS LANT DET Brunswick provides official telephone services to all Naval Air Station Brunswick commands and provides communications security material system (CMS) and electronic keying material system (EKMS) support to all base customers as well as Secure Telephone services to nine outlying customers covering five different New England states.

Additionally, NCTAMS LANT DET Brunswick provides Extremely High Frequency (EHF) satellite support to the submarine community via the EHF Polar Broadcast. Brunswick serves as one of only two sites designated to radiate this broadcast.

Many of the detachment's operations remain classified. What has changed over the years is the way the people who man NCTAMS LANT DET Brunswick accomplish their tasks and who does the work.

As far back as 1992, tactical support communications fell under the control of Naval Air Station Brunswick. That same year, Naval Computer and Telecommunications Command absorbed all Naval Telecommunications sites worldwide, including the tactical support communications centers, and Brunswick became a detachment of Naval Computer and Telecommunications Station Cutler,

ME. At that time, the staff consisted of 75 people, mostly military, in five departments.

In 2000, the detachment was outsourced and a contract was awarded to Rome Research Corporation for the operation and maintenance of the Tactical Support Communications Center. Four of the original five departments were abolished, along with all but two military billets. That same year, the detachment became a part of Naval Computer and Telecommunications Area Master Station Atlantic.

Today, the staff is down to 21 -- comprised of two Sailors, three DoD civilians and 16 contractors. What drove the staff reductions was improved technology and efficiencies. This caused a total manning concept change to occur, as the management of resources was tailored to continue operational support within new budgetary constraints.

"We used to man a bank of about 12 telephones," said Ross Lewis, a contracted telecommunications operator in the Tactical Communication Center. "Commands would call for their message traffic and we'd download it to them via modem. But in 2006, NCTAMS LANT took over messaging services support for all Naval Air Station, Brunswick commands to include this detachment."

Another of the Brunswick detachment's missions is to maintain the base telephone switch and monitor usage and billing. "This validation is made a lot easier these days by the two management software products used to collect and verify services," said Marge Severance, budget technician for the Base Communications Office.

In a little room at the back of their building, more telephone wires than anyone can seemingly count in a lifetime wind their way in colorful and orderly bundles around the room into several racks of electronic equipment before making their way

out of the building and around the base. While the room may appear confusing to most people, Bud Fallos, the detachment's telecommunications mechanic, will tell you the telephone switch is a revolutionary improvement from the one it replaced in 1994.

"The technology was so old. It was way past its time," he said. "There were no parts to be found for it and once a week, AT&T had to come down here to fix something or other on it." According to Fallos, once the switch was replaced, they went from 800 phone lines to more than 2,000 lines in two years. And gone were the days of waiting for a dial tone simply to place a call.

While many of the detachment's employees are looking for a new place to work as the date of the base closure approaches and VP-5 starts making the move to Jacksonville, FL, the base telephone switch will be maintained until the need for official telephone service.

Also operated and maintained is an unmanned receiver site located on the other side of the runways at NAS Brunswick. The receiver site contains 10 HF receivers remotely controlled by the Tactical Support Communications (TSCOMM). In years passed, it would have been manned 24/7. Seven antennas are used with these receivers, all located inside a 22-acre antenna field also maintained by this detachment.

Among other facilities the detachment maintains is their CMS account and high security vault which houses all the classified telecommunications security equipment and supporting material. As part of the detachment closure and official decertification of the vault all classified telecommunications systems equipment and material will be removed and relocated for use elsewhere within the Navy, and some equipment will be relocated to NCTS Jacksonville in support of the VP-5 squadron relocation.



(Left) Ross Lewis activates the Polar Broadcast on a USC-38. (Center) James Knight conducts a communications flight brief for VP air crew members. (Right) Harold Fallos (BCO) looks over continuity of telephone lines at the central telephone office. (Official U.S. Navy Photos)

Barritta keeps Base Communications Running

Story & photo by Muriel Smith, NCTAMS LANT

EARLE, NJ -- When the Base Communications Officer is busy at her desk, it's a sure sign that all the communications equipment and the cables keeping it functioning at the waterfront are in good working order. It doesn't happen often, but occasionally a problem arises that requires Nancy Barritta's on-site attention. That's because she believes in proactively taking care of the entire telecommunications network that keeps Naval Weapons Station, Earle, NJ, functioning and in contact with the rest of the world.

Nancy first came to Earle 28 years ago as a temporary key punch operator. She became a night time computer operator at a time when computers took up entire rooms. After that, she became a systems analyst, and when telecommunications was separated from Public Works in the early 1990s, she became director of the new Base Communications Office (BCO).

Her staff includes three technicians who respond to telecommunications emergencies, conduct regular inspections and perform routine maintenance on thousands of miles of wires and cables to keep the communications networks running smoothly and efficiently. That means, in addition to telephone lines and equipment, the BCO is also responsible for the fire and security alarm services, data circuits and the cable along Normandy Road that keeps waterfront and Main side connected at all times. At the waterfront, her BCO is also responsible for ensuring the

telecommunications system on the pier and to the ships in port functions properly.

"I like my job. I like working with my customers. I like knowing so many people and being in a position where I feel I'm helping the military," Barritta said.

In addition to ensuring all the lines and cables are in top working order, Nancy handles all the administrative

work for telecommunications, ensuring the bills to keep more than 1,400 lines functioning as well as coordinating with Public Works when there are problems with any phase of communications. She also interfaces with the Naval Computer and Telecommunications Area Master Station Atlantic Norfolk, VA.

"My job keeps me busy," she said with a smile.

When not at work, veterans and the military are still in her thoughts.

Nancy rode motorcycles as a teenager, and was lured back into riding by NWS Base Security Manager Pete Zaleski, also a bike enthusiast. When she learned Zaleski was also active in Rolling Thunder, an organization which promotes veterans' causes and works to raise awareness of MIAs and POWs, she was hooked again. Her husband is a Vietnam veteran

and her father served during the Korean conflict.

So, she and her husband joined Rolling Thunder. They're frequently seen with a half dozen or so friends taking day trips or simply riding around the Tinton Falls, NJ, area where they live.



Nancy Barritta

THE EVOLUTION OF NAVAL NETWORKS

OPERATIONAL CHANGES ON HORIZON

From NETWARCOM's NGEN Fleet Implementation & Transition Team

The Next Generation Enterprise Network (NGEN) is the Navy's largest Information Technology (IT) services acquisition program that is the follow on network to the Navy Marine Corps Intranet (NMCI) and will serve more than 800,000 users world-wide.

As the operational commander responsible for all Navy IT networks, operational transition falls under the responsibility of Commander, NETWARCOM, VADM H. Denby Starling II.

In 2008, Starling officially stood up the NGEN Fleet Implementation and Transition Team (FITT) as the responsible party for operational transition from NMCI to NGEN. The NGEN FITT is charged with serving two primary functions; first, supporting Navy's Echelon II commands ensuring effective transition from NMCI to NGEN; and secondly, in the development of the workforce, processes, and tools to support operational control of the network.

The NGEN FITT is organized to focus on strategic, operational and tactical functions to capture all areas of network operations required for this transition plan including the implementation of Global Network Command and Control structures for NGEN. Additionally, NGEN FITT acts as the NGEN communications lead (under NETWARCOM) for the Fleet.

Leading the NGEN FITT is CAPT Todd Rich who reported to NETWARCOM last September 2008. His team is charged with the specific mission to develop, maintain and promulgate a coordinated executable strategy to ensure effective transition from NMCI to NGEN while supporting the goals and objectives of the Naval Network Environment (NNE) strategy 2016. Highlights of these efforts include:

Development of the NGEN Network Operations (NetOps) Concept of Operations (CONOPS); a combined effort between NETWARCOM and Marine Corps Network Operations and Security Center (MCNOSC), Quantico, VA, outlining a concept of operations to provide the Navy and Marine Corps with increased management control and integration across all commands;

NGEN Security CONOPS which outlines the security concepts and

principles that will be incorporated into the design and operation of NGEN to ensure the protection and defense of NGEN assets, resources and data against both internal and external threats and vulnerabilities, with final approval expected in the second quarter of 2009;

Operational assessment of transition which identifies the critical activities required to migrate existing NetOps functions executed by the government and NMCI contractor to the NGEN construct;

Assessment of manpower requirements capturing an estimation of the required military and civilian members required to support the additional command and control required for NGEN; and most recently,

Command and control strategy document which defines the levels of command and control required to support operational control of the network.

To support the operational workforce required under NGEN, the NGEN FITT is working to define the roles and responsibilities of the Network Service Representative (NSR) in the form of a CONOPS. The CONOPS will outline the training and qualification requirements for the NSR workforce. The NSR is envisioned to be a newly established workforce in NGEN performing roles comparable with the existing NMCI Contract Technical Representatives (CTRs).

As a critical element in the success of NGEN, the current CTR roles must be understood and clearly defined. In January, the NGEN FITT hosted a two-day CTR/NSR workshop in Washington, DC. Chief Information Officers (CIOs) from various Echelon II commands sent their CTRs to meet and discuss a variety of topics including funding, tools, governance, and current workforce roles and responsibilities.

Members of NGEN FITT and Echelon II CTRs reviewed collective key take-aways from the two-day workshop. Attendees identified the need for fully integrated tools that will provide efficient end-to-end service-to-delivery, tracking,

maintenance, and invoicing. They also identified the need for development of processes to ensure integrity of data (seam management), and governance over the vendor(s). Efforts continue in the development of a NSR CONOPS with completion estimated for the fourth quarter of fiscal year 2009.

To achieve operational control across the Navy's IT enterprise, which consists of multiple service providers, the government is required to establish a strong core competency in IT Service Management (ITSM). To develop this competency, NGEN will have standard, repeatable ITSM processes based upon the proven concepts of the Information Technology Infrastructure Library (ITIL) version 3, a comprehensive and consistent set of best practices for ITSM which integrates business strategy with IT service strategy and allows organizations to address the increasing need to effectively manage IT resources.

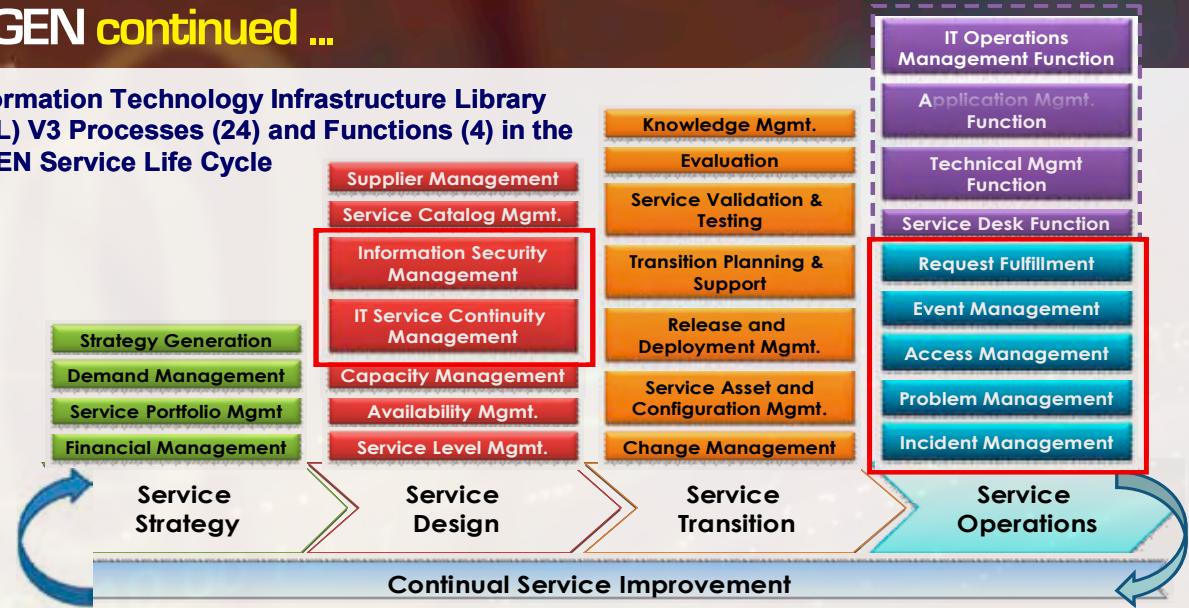
The NGEN FITT is charged with development of ITSM processes and development of an organizational construct to support increased operational command and control as part of an NGEN Early Transition Activity (ETA). The NGEN ITSM Process Development ETA collaborative team, started in March, is comprised of the ITSM Center of Excellence (ITSM COE) and the NGEN FITT.

The overall goal of this ETA is to develop and design repeatable ITSM processes that will provide NGENusers, operators and commanders at all levels with accurate and timely information which enables a shared understanding of the health and mission readiness of NGEN.

For the initial transition phase, the NGEN FITT is specifically focusing on developing the following seven processes: Event Management, Incident Management, Problem Management, Request Fulfillment, Access Management, Information Security Management and Information Technology Service Continuity Management.

As NGEN FITT continues to lay the groundwork for government oversight and operational control of the network, leadership continues to take full advantage of opportunities to communicate NETWARCOM's role in this endeavor. ✎

Information Technology Infrastructure Library (ITIL) V3 Processes (24) and Functions (4) in the NGEN Service Life Cycle



NGEN & Future of Naval Network Command & Control

From NETWARCOM Public Affairs Office

Eric Markland, deputy director, Next Generation Enterprise Network (NGEN) Fleet Implementation and Transition Team (FITT), recently discussed the future transition from Navy and Marine Corps Intranet (NMCI) to NGEN as the guest speaker at the April Armed Forces Communications and Electronics Association (AFCEA) luncheon.

Markland spoke about the upcoming role NGEN will serve.

"The NGEN baseline will include all the services offered on NMCI, while providing the Navy additional operational and design controls," he said. "NGEN forms the foundation for the Department of the Navy's future Naval Network Environment (NNE) that will provide secure, net-centric data and services to Navy and Marine Corps personnel."

Markland continued, "Navy owned and managed networks enable improvements in security; security that

is compliant with Joint/National Security Agency IA standards, giving us the ability to combat threats."

"With Navy owned networks, there will be an increased accountability for performance, as well as standardized business rules, infrastructure and architecture," he said.

"Another key element will be adaptability, including an enhanced responsiveness to increasingly dynamic requirements, allowing the incorporation of new technologies when and as required."

The NGEN FITT exists to develop, maintain and promulgate a coordinated executable strategy to ensure effective transition from NMCI to NGEN. Naval Network Warfare Command's role is to support the short and long term goals and objectives of the NNE 2016 strategy, as well as provide guidance and assistance to transition from NMCI to NGEN. NETWARCOM will also act as the NGEN stakeholder communications lead for the Fleet and will assist in supporting NGEN network operations (NetOps) requirements and capabilities.

In his closing remarks, Markland emphasized that starting with NGEN, the Department of the Navy is working toward implementing the NNE and that NETWARCOM is leading operational transition from NMCI to NGEN.

"Four major pre-transition efforts will affect NETWARCOM and its commanders," he said.

"These efforts will include the stand-up of the Global NetOps C2 structure for NGEN, the development of people, processes and tools for operational control, and the implementation of open standards for IT Service Management (ITSM) and employment of an industry-proven Information Technology Infrastructure Library (ITIL) framework."

"NETWARCOM and its commanders will retain operational command and control of the network under NGEN, with preparation starting now," Markland concluded.



(Center) Eric Markland, deputy director, NGEN FITT, speaks about the upcoming role of NGEN to conference attendees at an AFCEA luncheon. (Official U.S. Navy Photo)



Littoral Combat Ship Sailor Receives Copernicus Award

From PCU INDEPENDENCE (LCS 2) Public Affairs

Photo Illustration by Robin D. Hicks

NORFOLK, VA -- A member aboard the blue crew of Pre-Commissioning Unit (PCU) Independence (LCS 2) recently joined 29 other awardees at the Armed Forces Communications and Electronics Association (AFCEA) West Conference in San Diego to receive this year's Copernicus Award.

IT1(SW) Jon Antrim received the award in recognition of his accomplishments in information warfare.

"I'm extraordinarily proud to see one of my Sailors recognized with such distinction," said CDR Curt Renshaw, prospective commanding officer of Independence. "The LCS program attracts top performers in general, and for Antrim to distinguish himself in such esteemed company speaks volumes about his talent. We are extremely fortunate to benefit from his groundbreaking initiatives."

Antrim was the driving force behind the technical aspects of the littoral combat ship distance support Web system. He personally constructed a Hypertext Markup Language (HTML) coded web portal capable of capturing more than 900 operational and administrative requirements. His "one stop" multi-layered Web page will allow Independence Sailors to report a wide variety of essential data to shore-based support services without drowning the minimally-manned crew in paperwork.

Sponsored by AFCEA and the U.S. Naval Institute, the Copernicus Award is named after 16th century Polish astronomer Nicholas Copernicus.

Independence is the second littoral combat ship to be built for the Navy. The LCS is a fast, agile, mission-

focused platform designed for operation in near-shore environments, yet capable of open-ocean operation. It is designed to respond quickly and decisively to asymmetric "anti-access" threats such as mines, quiet diesel submarines and fast surface craft.



(Left to right) Antrim's wife, April, IT1(SW) Jon Antrim and CDR Curt Renshaw, PCO, PCU Independence (Blue) pose for a photo following Antrim's receipt of the Copernicus award. (Official U.S. Navy Photo)

NEW INSULATORS KEEP ANTENNA SYSTEM UP & RUNNING

Story by Jim Holmes, NCTAMS LANT DET Cutler

Photos by NAVFAC, SPAWAR San Diego Engineering Staff & NAS Brunswick NAA

Last November, the installation crew was cited in a Bravo Zulu message from Naval Network Warfare Command, which in part stated, "Conducting these actions concurrently resulted in an estimated savings to the Navy of more than \$750,000."

The Very Low Frequency (VLF) antenna system located at Naval Computer and Telecommunications Area Master Station Atlantic Detachment (NCTAMS LANT DET) Cutler, ME, exists to communicate with U.S. Navy submarines. The system is comprised of two tri-deco mono pole arrays. Each array is comprised of six panels.

These panels are suspended between 13,900-foot towers arranged in a star pattern for each antenna. The panels are electrically isolated from the ground utilizing safety core insulators, with a total of four insulators in each panel. Each tower has winches installed at its base which allows the antenna mechanics to lower each individual panel to the ground for maintenance.

In the mid 1990's the original insulators, each in excess of 30 years old, were replaced with oil-filled safety core insulators. Direct lightning strikes were causing a high rate of failure with the safety core insulators. Subsequently, Space and Naval Warfare (SPAWAR) Systems center, San Diego, made the decision to replace all of the safety core insulators with a new fail-safe porcelain string. The new fail-safe insulators were purchased in 2007 and the replacement of the safety core insulators commenced in the south antenna array in late July, 2008.

The new fail-safe insulator strings are approximately 57 feet long and comprised of 10 individual insulators. Each string must be assembled while in the field, utilizing heavy equipment and winches. A completed string weighs approximately 13,000 pounds. Conversely, the safety core insulators were 15 feet long weighing 3,000 pounds each.

The initial installation plan was developed by

NCTAMS LANT DET Cutler personnel with assistance from Naval Facilities Engineering Command and SPAWAR San Diego engineering staff.

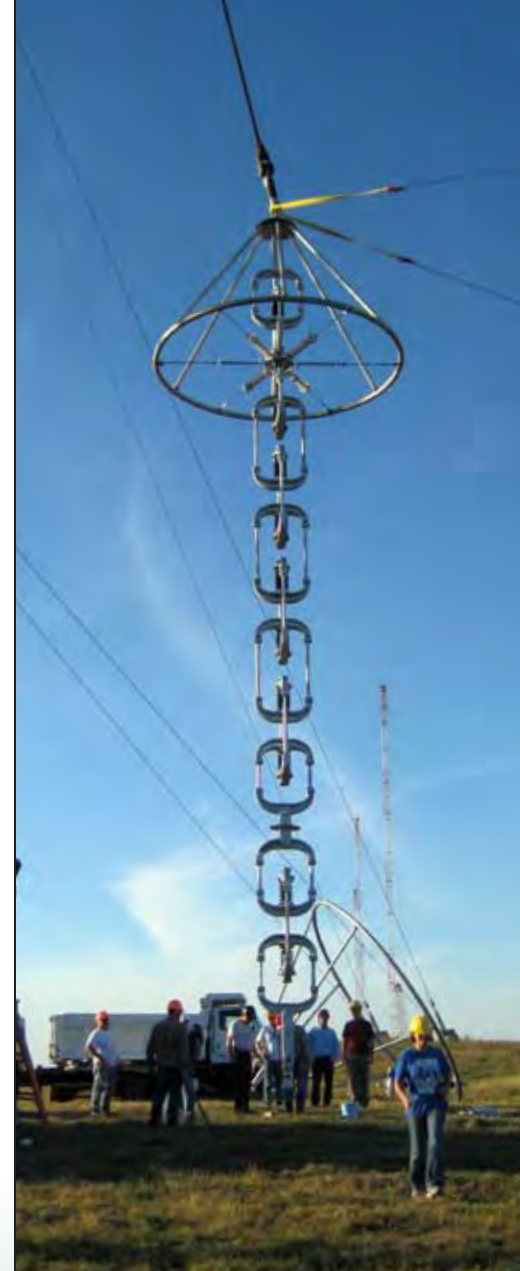
In the fall of 2007, the first of 24 insulator strings were assembled in the antenna field by the detachment's civilian antenna mechanics. The initial installation took 16 hours to complete. The procedure required 10 mechanics, two 15,000 pound winches, two category four cranes and one all terrain forklift, as well as numerous other pieces of heavy equipment.

After installing the first string of insulators, the installation procedures were evaluated, utilizing Lean Six Sigma principles. The evaluation process continued throughout the summer, which allowed minor changes to be made to the installation procedures. This included preassembly of some of the smaller components of the new insulator string and pre-staging of equipment and materials the day prior to each insulator replacement. These procedures significantly shortened the amount of time required to install each string.

By the end of the maintenance season, the antenna mechanics were installing two strings per week, each taking nine hours to install. Even with the intricacies of each evolution, weight of the components and the numerous pieces of equipment utilized for each insulator change, there were no injuries sustained.

NCTAMS LANT DET Cutler antenna mechanics were able to complete all normal routine maintenance on both antenna systems -- approximately 13,000 man-hours total -- as well as installing 18 fail safe insulator strings in the south antenna during the 2008 summer maintenance season.

Insulator components for the north antenna system were received this past fall. Installation of the north antenna insulators is currently scheduled for the 2009 antenna maintenance season which began recently and runs through the last week in October.



(Background) NCTAMS LANT DET Cutler, ME. (Clockwise from left) Antenna Riggers assemble one of 10 insulator links that make up the fail-safe insulator chain. Riggers install a large corona ring located in the background. A completed fail-safe insulator string.

NCTAMS Det San Diego, NETWARCOM set DUI-Free Standard

By MC2(SW) Christopher J. Koons



(Left to right) ITCs Matthew Stevens, Derrick Hein, Lugene Tyson, MaryJane Ramos, LT Henry Martinez II, ITCs Lana Tullos, Richard Rivera, Andre Belser and Nick Balich: NCTAMS Hawaii's DUI-Free Standard team. (Official U.S. Navy Photo)

Although driving under the influence of alcohol (DUI) incidents remain a national problem, one Navy command has used a combination of good leadership and sound policies to go more than 900 consecutive days without a DUI incident involving any of its Sailors.

Naval Computer and Telecommunications Station, Navy/Marine Corps Intranet (NMCI) Detachment San Diego began its streak of DUI-Free days Oct. 29, 2006, and reached its 900th day on April 16th of this year. According to LT Henry A. Martinez, the detachment's officer-in-charge, the main credit for this accomplishment goes to the command's deckplate leadership.

"This great accomplishment could not have occurred without the 'intrusive leadership' of LCDR Donald C. Hendrix, our previous OIC, our Chief's Mess, our leading petty officers and all of us realizing the importance of having a plan and staying with it," said Martinez. "Our chiefs and LPOs constantly reinforce responsible behavior, and they ensure all of their Sailors have their home and cell phone numbers in case they find themselves unable to drive."

To ensure that Sailors know right away what the command's policies are on alcohol abuse, training begins as soon as they arrive at the detachment on what is expected of them, Martinez explained.

"They are briefed on responsible drinking, as well as making and following a good liberty plan," he added. "They sign a service record 'Page 13' entry to document this training. Additionally, the senior enlisted leader talks one-on-one with each of them and re-emphasizes the importance of responsible drinking and proper conduct while on liberty. He makes everyone aware that

if all else fails, they should call the command duty officer or the quarterdeck, and the duty driver will pick them up, or use their 'Arrive Alive' cards to call a taxi."

The cards are given to Sailors to use if they should happen to be drinking and need a taxi, but have no money for the ride. The taxi company bills the command and the Sailor reimburses the command by his or her next pay period.

"Part of this process involves informing Sailors of the consequences of being charged with DUI," said Martinez.

"We tell them that they will go to Captain's Mast and receive the maximum punishment allowed," he said. "We also discuss the overall cost of a DUI, which includes the possible loss of one pay grade, and the pay they may lose during the time it will take to 'start over' in that lower pay grade and retest for the next one. When Sailors hear that the cost could end up being more than

\$10,000, they realize a cab ride is much cheaper."

Additional costs include increases in insurance premiums, possible vehicle repairs if in an accident and loss of security clearance.

"For many junior Sailors, it is the sense of shame they will feel in the eyes of their peers that is the biggest deterrent to drinking and driving," Martinez explained.

"In addition to wanting to do the 'right thing,' peer pressure has been one of the biggest drivers for our Sailors," he said. "No one wants to be 'The Sailor' who makes the front gate ticker go back to 'Zero Days since the Last DUI.' This is a great case of positive peer pressure."

In addition to NCTAMS Det. San Diego's accomplishment, in April, Naval Network Warfare Command (NETWARCOM) headquarters also reached the milestone of going a year without a DUI, which some of its leaders also credit to sound policies.

"Whenever we have special events

such as holiday stand-downs and the command holiday party, we go out of our way to stress the importance of not consuming alcohol before you get in your car to drive," said ITCS(SW/AW) Daniel Claycomb, NETWARCOM's Drug and Alcohol Program Adviser. "We hold Alcohol-Aware classes and put up posters around the command warning Sailors not to drink and drive. The most important part is when LPOs inform their subordinates about the dangers of driving under the influence."

To support the Navy's efforts to combat drunk driving, Claycomb said that Sailors should log on to <http://www.thatguy.com>, which contains tools and advice to warn people about the dangers of alcohol abuse.

"We must continually put the word out at the appropriate times about the consequences of DUI using both written and verbal communications," said Claycomb. "We can't let our guard down now, because if we do, we'll start having problems." ✂

NIOC Hawaii wins Blood Donation Award

From NIOC Hawaii Public Affairs



We frequently hear the phrase "support to the warfighter." Navy Information Operations Command (NIOC) Hawaii does just that every day. One non-mission way that NIOC Hawaii has supported the warfighter is by donating blood.

The Armed Services Blood Program (ASBP) comes to Kunia four times a year. ASBP Blood Donor Recruiter, Michele Lele said, "Kunia is one of the best stops of all the places we go. The response and support here is superb."

Donation days are normally busy ones for the people taking the donations. As further proof of the support given by the Kunia community, the command was recently recognized as the installation with the highest blood donor participation per capita for the state of Hawaii.

"We normally collect 50-75 units of blood at each of our stops," Lele said. "The last time we were here we collected 80 units, and by the looks of things we'll collect that much again."

ASBP personnel collect five tubes of blood from each donor, which is immediately placed in an ice box. The blood is then transferred to the lab at Tripler Medical Center where it is screened. Of the 80 units collected at Kunia, approximately 40 will be shipped off to Iraq and Afghanistan to support troops on the ground in harms way. The remaining 40 units are kept at Tripler for surgery patients.

NIOC Hawaii Commanding Officer, CAPT Jim Hagy said, "Our participation most likely saved lives and will continue to do so in the future. Thank you for your support and participation. Great job, well done." ✂



NCDOC gets Model Partnership Award

Story & photos by MC2 Adrian T. White

VIRGINIA BEACH, VA --- Volunteers from the Navy Cyber Defense Operations Command (NCDOC) were recently awarded the 2008-2009 Model Partnership of the Year Award for helping enhance instructional programs and fostering positive, supportive relationships at Bayside Elementary School.

NCDOC Sailors volunteer as tutors and mentors, offering academic assistance and serving as positive role models to students. They participate and help manage special events, such as the Book Fair, Fall Festival and Reading Night, and participate in and help manage various activities. The school benefits because these Sailors encourage high levels of achievement and excellent behavior from Bayside's students.

"Working with the kids was a very rewarding experience," said NCDOC Partnership and Education Coordinator, YN2 Victoria Scott. "It was an honor to be

a part of their lives. It felt great to be recognized as a representative of the Navy, NCDOC and as a positive role model."

First-grade teacher Leatha Fischer writes, "Always ready to do any task, the volunteers are kind, enthusiastic and diligent. Keeping the children as a focus, the volunteers are devoted to helping the students succeed. The joy and excitement that the students express when spending time with their mentors is a testament to the positive impact that this partnership has on our students."

The Virginia Beach City Public Schools (VBCPS) Partnership Advisory Link, which began in 2001-2002 as an advisory body made up of school and community representatives, recognizes Model Partnerships annually at the VBCPS Partners in Education Appreciation Breakfast. ✂



(Above) YN2 Victoria Scott, an NCDOC Sailor, mentors to a group of elementary students at a local school. (Left) CT3(SW) J'mese White, also from NCDOC, reads to local elementary school students. Both Sailors are part of NCDOC's award winning mentorship program in Virginia Beach, VA.

NIOC Hawaii FRG, Ombudsman, support Sailors & Their Families

By LTJG Carrie K Sanders, NIOC Hawaii PAO

With the largest single command in the state of Hawaii, some might find the task of serving as Family Readiness Group (FRG) president or command Ombudsman daunting, but you wouldn't know it by meeting with Felicia Fernandez, Tammy Bruce or Terry Marcus.

These three ladies are driven by their dedication to Navy Information Operations Command (NIOC) Hawaii, families, and consider their efforts as a service to those who serve. When asked about the FRG's family friendly orientation, Fernandez the FRG president said, "We are not just family-friendly, we are Sailor-friendly. Anything we do is for single Sailors as well as those with families."

At a recent FRG meeting, they discussed the events they have planned for the upcoming months.

NIOC Hawaii FRG and Ombudsman published the first edition of "NIOC News." In March,

NIOC Hawaii FRG co-hosted a car wash along with the command's Navy Day Ball committee to raise funds to help pay for the ball and other family events. The car wash was at the Fleet Reserve Association.

Some of the money from the car wash paid for the 2009 Bunny Hop, FRG's largest event of the spring. During the Bunny Hop, children of all ages hunt for Easter eggs and enjoy some great food offered by the other organizations within NIOC Hawaii. FRG also offered face painting, bounce houses and pictures with the Easter Bunny himself.



The Bunny Hop and car wash are not the only events on the FRG and the Ombudsman plan. Still ahead this year are a family bowling night, a Kids' Birthday Party at a local transitional family shelter and a family-in-need donation station for Sailors of babies and small children that lack some basics such as clothing and toys.

But, the most important issues for the FRG and Ombudsman are family issues. They are available 24 hours a day to Sailors, spouses and children alike who need help when times are tough, when life simply gets to be a bit much, when preparing for deployment, trying to work with shift work or just dealing with life in the Navy.

When asked why the family readiness group does all it does, Marcus said, "Because taking care of the Sailors' family allows the Sailor to concentrate on his or her mission." ✂



(Above) Members of NIOC Hawaii's Family Readiness Group and Ombudsman share ideas during a weekly meeting. (Official U.S. Navy Photo)

Naval Intelligence Training Center honors Legends

LCDR William Bunn, NMITC Public Affairs

VIRGINIA BEACH, VA -- Memorials honoring two historic legends in the naval intelligence community were dedicated May 1 at the Navy and Marine Corps Intelligence Training Center (NMITC), at Naval Air Station (NAS) Oceana, Dam Neck Annex.

The memorials commemorate the lives and contributions of CAPT Frank P. Notz and CDR John "Jack" Graf. The NMITC auditorium was standing room only during the ceremony, which was attended by members of both the Notz and Graf families.

In addition to the memorials, the newly renovated Hall of Excellence chronicling the history of naval intelligence through decades of changing warfare was opened for viewing.

Notz, a former commanding officer of NMITC and mentor to a generation of intelligence officers before he passed away in 1999, had a student library named in his honor at the event. Notz' wife, Belinda, expressed her sincere gratitude as she toured the new Frank Notz student library.

"Everything...the words, the memorial, everything...is just perfect," she said.

CDR Jack Graf was a naval intelligence liaison officer assigned to Navy Intelligence Field Organization Vietnam. He was shot down while on a reconnaissance mission, captured and held as a POW. Graf was tortured and later killed while attempting to escape. Now every staff member, student and visitor to NMITC will pass by the CDR Jack Graf memorial near the NMITC quarterdeck.

Graf's niece, Judy Connors, and her family attended the ceremony.

The dedication's keynote speaker was VADM David J. "Jack" Dorsett, director of naval intelligence.

Discussing Notz' character and accomplishments during 30 years of naval service, Dorsett said Notz "freely gave of his time and knowledge to the next generation...my generation...and for that, we are humbled and grateful."

In his comments regarding Graf, Dorsett noted the captain's "honor and courage in the face of unimaginable hardship." Dorsett quoted former Director of Naval Intelligence VADM Earl Rectanus, who stated "there has never been a naval intelligence professional who has demonstrated the concepts of courage, dedication and sacrifice more than has Jack Graf."

The theme of the ceremony was "Honoring the Past and Embracing the Future of Naval Intelligence." During her remarks, current NMITC Commanding Officer CAPT Elizabeth Train tied the actions and contributions of Notz and Graf to the challenges the newest generation of young intelligence professionals face.

"When our students leave this schoolhouse, they do so knowing they will serve in harm's way, fully integrated into warfighting operations -- whether on board an aircraft carrier, a large deck amphib or other combatant, or assigned to expeditionary or special warfare units

operating in littoral and riverine environments," declared Train.

As he closed his remarks, Dorsett noted that the torch of responsibility once held by Notz and Graf was now in the hands of those intelligence professionals in attendance.

"It's now time for you to write the next chapters of our history...through your lives, well-lived, and duty served honorably." ✂



(Above) CDR John Graf with his family.

(Below) CAPT Frank Notz. (Official U.S. Navy Photos)



Command awards Chief for Actions

Story & photo by LTJG Carrie Sanders, NIOC Hawaii Public Affairs

For most Sailors, going to see the Captain at Mast is a fearsome moment, one that comes after failure to obey a direct order or other violations of the Uniform Code of Military Justice (UCMJ). However, for CTRC(SW) Larry Dewayne Bates, the visit was a welcome one as he was in receipt of a Meritorious Mast. Meritorious Mast is something most Sailors only hear about. This was Bates' second.

In mid-February, Bates attended the command's daily operations brief. Immediately following the brief, he was directed to report for Captain's Mast. An unassuming chief stood shaking nervously as he took his place in front of CAPT James Hagy, commanding officer of Naval Information Operations Command Hawaii.

The events leading up to the mast were, to Bates, simple. He said, "I did what Chiefs are supposed to do -- take care of Sailors," he said. To the command, however, he went above and beyond.

His citation read ... "In only a few short months, Chief Bates demonstrated superior leadership and mentoring to more than 40 junior enlisted Sailors and bestowed his practical senior enlisted knowledge upon 20 junior officers. He quickly established himself as division leading chief petty officer while remaining on the watch. His inspirational leadership enhanced productivity and morale amongst his Sailors, fostering an innovative environment. He has continued to bring the Fleet Information Operations Center (FIOC) closer to a global concept by enhancing communications in and out of the Pacific theater. His efforts have allowed FIOC Hawaii to further support the Commander Pacific Fleet's tactical consumers by strengthening relationships with fleet commanders and National Intelligence Community partners."

Bates has served in the Navy for 20 years. When asked about the event, his only reply was, "I am humbled to receive such an honor -- it was a complete surprise." ✂





BRONZE STAR

LCDR Sherri Mitchell, Multi-National Corps-Iraq



DEFENSE MERITORIOUS SERVICE MEDAL

LT Danny Bouie, Int Security Assistance Force
CTRC Philip Gonzalez, 2nd Stryker Cav Regiment
CDR Kevin Hinton, NIOC Maryland
CTN1 Matthew Lamirande, NIOC Maryland
LCDR Brad Melichar, NIOC Maryland
LT Richard Moore, NIOC Maryland
CTT1 Kurt Sauer, NSA/CSS
CTIC Dmitriy Sokol, NIOC Texas
CAPT Timothy White, JFCC
CTIC Vincent Whitmire, NIOC Maryland



MERITORIOUS SERVICE MEDAL

LCDR Donald Hendrix, Jr., NMCI Det San Diego
CDR Kevin Marshall, NR NIOC Camp Parks
CDR Robert McGaha, NIOC Maryland
CTICM Bradley McNamar, NETWARCOM Norfolk
CMDCM Daniel Miller, NIOC Maryland
CWO4 Joseph Nalley, NCTAMS PAC Wahiawa
LCDR Thomas Sanchez, NETWARCOM Norfolk



AIR MEDAL

CTT1 Jason Kappel, NIOC Bahrain
CTI1 Christopher Mullins, NIOC Bahrain
LT Tabitha Wright, NIOC Bahrain



JOINT SERVICE COMMENDATION MEDAL

IT1 Renee Boulton, NIOC Maryland
CTI1 Heather Cassity, NIOC Maryland
CTN1 Derek Christensen, NIOC Maryland
CTI2 Marie Combs, NIOC Maryland
CTR1 Joshua Dufault, Joint Task Force
LTJG Donna Gilbert, NIOC Maryland
CTR2 Adam Hahn, NIOC Misawa
CTR1 Alexander Hokanson, Joint Task Force
CTN1 Shawn Homan, NIOC Maryland
LT Lemuel Lawrence, JFCC for Network Warfare

CWO3 Deborah McCrayer, NIOC Maryland
LTJG Rhea Mortam, NIOC Maryland
CTM1 Trevor Pashenee, NIOC Maryland
CTI1 Benjamin Sheldon, NIOC Maryland
CTI1 Ruth Simmons, NIOC Maryland
ITC Latwaine Sweeper, Headquarters, JTF
CTI2 Michael Thorne, 4th Infantry Division
IT2 David Zunac, NIOC Maryland



NAVY AND MARINE CORPS COMMENDATION MEDAL

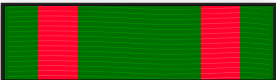
CTR1 Patricia Acevez, NIOC Suitland
ITC Anna Allegretto, CID-ARI Corry Station
ITC Neil Apresto, NCTS Guam
CTR1 Ryan Astle, NIOC Maryland
IT1 Nii Banfro, HQ NETWARCOM Norfolk
CTNC Kirk Berka, NIOC Pensacola
CTIC Anthony Bolouri-Rad, NR NIOC Georgia
LCDR Sean Brandes, NIOC Texas
CTNC Robert Brashear, NIOC Pensacola
CTICM Robert Buelow, NR NIOC Great Lakes
CTICM Robert Buelow, NR NIOC Fort Gordon
ITCS Curtis Campbell, NETWARCOM Norfolk
LT Sharon Cannon, NETWARCOM Norfolk
YNCM Donald Carter, NIOC Georgia
CTI1 Armando Castro, NIOC Hawaii
LTJG Eren Cataloglu, NIOC Yokosuka
LTJG Benjamin Collins, NIOC Suitland
ITC Suzanne Davis, NCMS Washington, DC
LCDR Christine Devries, NETWARCOM Norfolk
CTNC Shante Dill, NIOC Suitland
CTR1 Charles Dodd, NR NIOC HAWAII
CTRC Michael Dugan, NIOC Georgia
LT Erich Fassett, NETWARCOM Fort Meade
YN1 Kimberly Ferguson, NIOC Georgia
IT1 Edwin Flores, NCTAMS PAC Wahiawa
ITCS Tracy Floyd, NCTS Bahrain
CTTC Christopher Giffing, NIOC Georgia
ET1 Christopher Goodyear, NCTS Naples
CTR1 Andrew Griffiths, NIOC Texas
CDR Maurice Harper, NR NETWARCOM HQ Norfolk
YN1 Lisa Hartman, NIOC Maryland
LT Dana Heidenescher, NCTAMS PAC Wahiawa
ITCM Michele Hermosura, NCTAMS LANT Det HR
CTI1 Walter Hernandez, NIOC Georgia
LCDR John Hudson, NIOC Maryland
CTT1 Jerome Hughs, NIOC Georgia
LT Evan Huyettearrizza, NIOC San Diego
LTJG Nicholas Jensen, NIOC San Diego
CTN1 Joseph Johnston, NIOC San Diego
IT1 G. Jones, NCTAMS PAC Wahiawa
CTNC William Katz, NIOC Pensacola
CTI1 Erich Keough, NIOC Misawa
LT Brian Kristan, NETWARCOM Norfolk
CWO2 Robert Long, NIOC Georgia
LT Robert Marnell, NR NIOC Orlando
LT Reshonda McKee, NETWARCOM Norfolk
CTRC Kenneth Meadows, Jr., NIOC Yokosuka
ITC Brian Meyer, NETWARCOM Norfolk
ITC Tyrell Mitchell, NCTS Naples
CTN1 Eric Nelle, NCDOD Norfolk
LCDR Dorothy Nguyen, NR NIOC Camp Parks

LT Tony Nichols, NCTS Far East Det Diego Garcia
CTTC Vaughn Okuna, NIOC San Diego
CTRC Joseph Piwonski, NIOD Brunswick
CTRC Nicholas Prebeg, NIOC Georgia
CTI1 Taro Radke, NIOC Misawa
ET1 Matthew Reed, NCTS Naples
LT Tracey Rhone, NCTAMS PAC Wahiawa
CTNC Peter Russo, NR NIOC Fort Worth
IT1 Annette Salas, NIOC San Diego
ITC Kelvin Shubert, NETWARCOM Norfolk
CTIC Jared Smith, NIOC Georgia
CTMCS Roger Spillane, NETWARCOM Norfolk
ETCS Ronald Stewart, NCTS Bahrain
CTRC Jonathon Stone, NIOC Whidbey Island
CTICS Michael Sykes, NIOC Bahrain
LCDR Nathaniel Sylvester III, NIOC Suitland
ITC Paul Taylor, NETWARCOM Norfolk
CTR1 Stefanie Tignor, NIOD Chesapeake
CTN1 Brian Waggoner, NIOC Texas
IT1 Mark Watson, NCTS Naples
EN1 Michael Watson, JMAST PAC Aurora
CTI1 Aimee Wiensz, NIOC Misawa
CTT1 Matthew Wilber, NIOC Georgia



JOINT SERVICE ACHIEVEMENT MEDAL

CTR2 April Connor, NSA/CSS
CTR1 Philip Eickholt, NIOC Maryland
CTR3 Bethany Eigenfeld, NIOC Maryland
CTR3 Eric Girard, NIOC Maryland
CTI2 Bettina Haper, NIOC Texas
CTI3 Kelsey Hillis, NIOC Maryland
CTN1 Aaron Jolly, NIOC Maryland
CTI2 Zachary Marion, NIOC Texas
IT3 Sean McCormick, NIOC Maryland
CTI1 Benjamin Musson, NIOC Georgia
CTN1 Kevin Siegers, NIOC Maryland
CTR1 Jennifer Valentin, NIOC Maryland
CTN2 Leo Zerhusen, NIOC Georgia



NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

IT1 Juan Acala, NCTS Sicily
CTI1 Miguel Acosta, NIOC Texas
IT1 Robert Ader II, NIOC Suitland
CTR1 Daniel Adkins, NIOC Yokosuka
IT2 William Adkison, NETWARCOM Norfolk
ITCS Deborah Alexander, NCTS San Diego
CTI1 William Alexander, NIOC Georgia
CTM2 Carlos Alvarez, NIOD Groton
IT1 Sedwick Antoine, NCMS Det San Antonio
CTI1 Sean Aschoff, NIOC Georgia
CTN2 Benjamin Austin, NIOC Pensacola
CTR2 Adam Baker, NIOC Georgia
IT1 Nii Banfro, HQ NETWARCOM Norfolk
CTR1 Kimberly Barth, NIOC Whidbey Island
CTR1 Timothy Becker, NIOC Hawaii

ET2 Brittney Bisping, NCTS San Diego
IT2 Yoncenia Black, NCTAMS LANT Norfolk
CTR2 Bradley Bock, NIOC Hawaii
CTT2 Stephen Bramer, NIOC Hawaii
IT2 Matthew Brashares, NCMS Det Fort Huachuca
ET2 James Brown, NCTS Bahrain
IT1 William Brown, NCDOD Little Creek
IT1 Katisha Burns, NCTAMS LANT Det Rota
IT3 Lindsay Caldwell, NCTS San Diego
IT1 Martha Call, NCTS Guam
IT1 Crystal Campos, NMCI Det Norfolk
SK2 Lalyn Carabeo, NIOC Hawaii
CTR1 Cameron Chadd, NIOC Whidbey Island
IT1 Lisa Childress, NCTS Bahrain
CTN1 Daniel Chubb, NCDOD Little Creek
IT1 Colleen Cofield, NCTAMS LANT NMCI Det Norfolk
IT2 Kyle Cooley, NIOC Whidbey Island
CEC Michael Cortez, NCTS Naples
ET1 Richard Crowder, NCTS Bahrain
ET1 Catherine Cruse, NCTAMS LANT Det Rota
ET2 Victor Cruz, NCTS Bahrain
IT1 Alison Czuhajewski, NIOD Groton
IT2 Seng Dara NCTS San Diego
IT1 Nathan Dartnell, NETWARCOM Norfolk
IT1 Valencia Dawson, NCTS Bahrain
IT1 Tammy Dean, NCTAMS LANT Det Brunswick
CTR2 Santiago Delgado, NIOC San Diego
IT3 Tamara Dempsey, NCTS San Diego
YN1 Jenean Dickens, NCTS San Diego
IT2 Jonathan Donate, NIOC Yokosuka
IT1 Deyan Dontchev, NMCI Det San Diego
ET2 Joshua Drum, HQ NETWARCOM Norfolk
IT1 Andrew Duerre, NCTS Sicily
CTI1 Carrie Duncan, NIOC Maryland
CTR2 Charles Dye, NIOC Hawaii
CTIC Josef Edmunds, NIOC Hawaii
ITSN Tashika Enwright, NCTAMS LANT Norfolk
YN2 Seanna Espinoza, NIOD Groton
MA3 Ryan Evans, NIOC Sugar Grove
CTTC John Farrell, NR NIOC Fort Dix
IT1 Anthony Fattizzi, NCDOD Little Creek
CTI1 Ashley Freeman, NIOC Bahrain
IS2 Jason Gilkey, NETWARCOM Norfolk
CTT1 Natasha Glover, NIOC Yokosuka
CTN2 Larry Goings, NIOC San Diego
CTN2 Anthony Gonzales, NIOC San Diego
ET2 David Gonzales, NCTAMS LANT Norfolk
YNC Antonio Green, NCTS Bahrain
ET2 Nathan Green, NCTS Naples
ET2 Neal Green, NCTS SD SCU Det Patuxent River
IT2 Kyle Griffin, NCTS San Diego
CTR2 Zachary Gross, NIOC Suitland
CTN2 Adam Hardin, NIOC Pensacola
IT2 Jason Harris, NCTS Bahrain
ITCS Jamal Headen, NETWARCOM Norfolk
EN1 Coby Henderson, NIOC Norfolk
CTT2 James Henry, NIOC Texas
IT3 Clifford Hensley, CID-ARI Corry Station
IT3 Patrick Hillers, NCMS Washington D.C.
ITCS Ernest Hoffman, NMCI Det Norfolk
IT2 Patrick Honvo, NCTS SD SDU DET Patuxent River
CTT1 Clifford Howe, Jr., NIOC Texas
CTR1 Rebecca Hubenak, NIOC Georgia
IT2 Cleodis Johnson III, NIOC Norfolk
ET1 Joseph Johnson, NCTS Bahrain
ET2 Cedric Jones, NCTS Jacksonville
IT2 Danielle Jones, NCTAMS LANT Norfolk
IT2 Lakiesha Jones, NCTAMS LANT Det HR

IT2 Shermaine Jones, NCTS Bahrain
ITC Johnny Joseph, NIOC Yokosuka
CEC Keith Kahn, NIOC Bahrain
LT Stephen Kantz, NIOC Misawa
IT1 Richard Kay, Jr., NMCI Det San Diego
IT1 Steven Kelley, NCTS Jacksonville
ET2 Patrick Kramer, NCTS San Diego
ET2 Michael Krebs, NCTS Bahrain
ITC Jacob Kuehl, NCTAMS LANT Det Rota
IT1 Paul Kunkle IV, NCTAMS LANT Det Rota
CTN1 Melanie Labbe, NCDOD Norfolk
CTR1 Richard Lepley, NIOD Chesapeake
MC1 Corey Lewis, NETWARCOM Norfolk
CTI2 Lili Lissia, NIOC Bahrain
IT2 Justin Longfellow, NCTS SD SCU Det PAX River
IT3 Luis Lynch-Maldonado NCTS Naples
ITC Rolando Macapagal, NCTAMS PAC Wahiawa
ET3 Jay Maltry, NCTS Bahrain
IT2 John Martin, NIOC Norfolk
CTR1 Shannon Martin, NIOC Georgia
CTI1 Jonathan Martin, Jr., NIOC Georgia
LT Michael McCarthy, NIOC Misawa
ET2 Christopher McClearse, NCTS Bahrain
CTI1 David McGehee, NIOC Bahrain
ET2 Thomas Mebane, NCTS Bahrain
LTJG David Meland, NCTS San Diego
IT1 Osvaldo Melendez, NCMS Washington DC
LT Vincent Mettle, NR NIOC Fort Meade
CTR1 John Miculka, NIOC Whidbey Island
IT2 Graig Miller, NMCI Det San Diego
CTR1 Kip Miller, NIOC Misawa
IT1 Jermaine Mims, NCTAMS LANT Det Rota
CT1 Barry Mingo, NCTS Sicily
ITC Shawn Moorefield, NCTS Naples
ETC Kailars Morgan, NCTS Bahrain
ET2 Pleas Morton, NRTF NISCEMI
CS2 Daniel Muggelberg, NIOC Maryland
CTR2 Sean Mullen, NIOC Hawaii
CTI1 Artem Murodov, NIOC Georgia
CTR1 James Newsome, NIOC Georgia
IT3 Patrick Nguyen, NCTS Sicily
CTR1 Anna Nichols, NIOC Georgia
CTT2 Tiffany O'Connor, NIOC San Diego
ET2 Cameron Oetjen, NCTS Sicily
IT2 John Olson, NETWARCOM Norfolk
IT1 Angel Ortiz, Jr., NCTAMS LANT Det Rota
IT1 Phineosjay Oshio, NCTAMS LANT Det Souda Bay
ITC Chad Overly, NIOC Georgia
IT2 Jeffrey Palyakov, NIOC Suitland
ET2 James Parker, NIOC Norfolk
IT1 Jennifer Pate, NCTAMS LANT Det HR
ET2 Blaize Pearson, NCTAMS LANT Det Rota
ET2 Julio Pedroza, NCTAMS PAC Wahiawa
IT1 Jose Perez, NCTS Bahrain
YN3 Kyle Perkins, NIOC Sugar Grove
IT1 Rodolfo Pizarrocruz, NCTS Bahrain
YN1 Jacqueline Polanco, NR NIOC Orlando
CTM1 Anthony Radzimoski, NIOC Pensacola
MA3 Markus Ramsey, NIOC Sugar Grove
CTR1 Heidi Rankin, NIOC Hawaii
ITCS Kevin Ratcliffe, NCTS Naples
IT3 Philip Raymond, NCMS Washington D.C.
ET2 Samuel Renfrow, NCTAMS PAC
CTT1 William Richards, NIOC Georgia
IT1 Marquis Richardson, NCTS Bahrain
CTR1 Ryan Robinson, NIOC Yokosuka
IT2 Cynthia Rodriguez, NIOC Norfolk
IT1 Douglas Rogers, NCTAMS LANT Norfolk

IT2 Paul Schooley, Jr., NIOC Yokosuka
CTIC Seth Schrawyer, NIOC Misawa
CTN1 Jeremy Scott, NIOC Pensacola
YN2 Victoria Scott, NCDOD Norfolk
IT1 Sarah Sendrey, NCTAMS LANT
CTI1 Tyepha Senvisky, CENINFODOM Fort Meade
CTR1 James Shaver, Jr., NIOC Whidbey Island
IT3 Jung Shin, NCTS San Diego
CTT1 Sean Sill, SPECBOAT TEAM TWO ZERO
CTI1 Andra Simpson, NIOC Georgia
IT2 Michael Singletary, NCTS Bahrain
CWO3 Avalyn Smith, NCTAMS LANT Norfolk
CTM2 Jon Smith, NIOC Norfolk
ET1 Brian Solomon, NCTS Bahrain
ET2 Scott Sonnier, NCTS Bahrain
YN2 Jeremy Spence, NETWARCOM Norfolk
CTR2 Juniel Spruiel, NIOC Hawaii
ET2 William Stalter, NRTF NISCEMI
ET1 Janusz Swierczewski, NCTS Bahrain
ET2 Peter Tang, NIOC San Diego
IT2 Vincent Tarantini, Jr., NCTAMS LANT Norfolk
MC2 Christopher Thamann, NIOC Sugar Grove
CTI1 Jamie Thorn, NIOC Texas
CTR1 Jennifer Tiberii, NIOC Georgia
IT1 Monica Tipton, NCMS Washington D.C.
IT3 James Tormey, NIOC Maryland
SKC Edward Townsend, Jr., NCTAMS LANT
LTJG Samuel Trassare, NIOC Georgia
IT1 Sonia Trotter, NCTS Guam
ET1 Richard Truchanowicz, NCTS Far East Yokosuka
CTR1 Jeremy Turnbull, NIOC Whidbey Island
CTM1 Brian Underwood, NIOC Yokosuka
CTR1 Zachary Urban, NIOC Misawa
IT1 Jennifer Utley, NCTAMS LANT Det HR
EO2 Arcello Venzon, NIOC Hawaii
CTN1 Theresa Verity, NIOC Pensacola
IT1 Danny Vines, NRTF NISCEMI
UT2 Jeffery Walter, NIOC Hawaii
CTIC Giselle Wells, NIOC Texas
ET2 James West, NCTAMS PAC Det Whidbey Island
CTN1 Latonya White, NIOC Hawaii
ET1 Ronald White, NCTS SD SCU Det Ok City
IT2 Allen Whitehurst, NCTAMS LANT Det HR
ET1 Anthony Williams, NCTS Sicily
IT1 Sparkle Williams, NMCI Det Norfolk
CTT1 William Wood, NIOC Hawaii
ET1 Breeze Woodall, NCTS Sicily
IT3 Clayton Woodruff, NCTAMS PAC Wahiawa
CTI1 Raymond Woods, NIOC Maryland
ETC Douglas Yennie, NCTAMS LANT Det Rota
CTR2 Brandon Young, NIOC Suitland
IT1 Jefferson Youngblood III, NCTS Bahrain
CTR1 John Yzenbaard, NIOC Whidbey Island
IT2 Hailey Zaiden, NCTS San Diego
ET1 Adrian Zellander, NCTAMS LANT Norfolk
CTT2 Jennifer Zolnik, NIOC San Diego



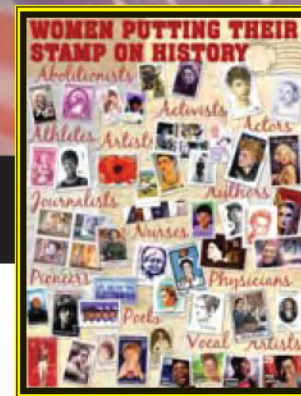
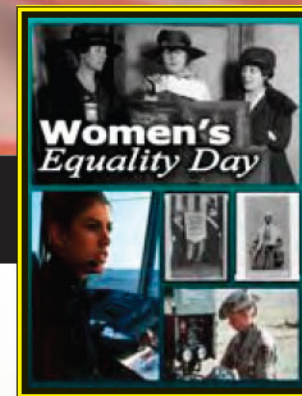
MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL

IT1 Carlos Barnes, NCTAMS LANT Det GITMO
YN2 Antoinette Bush, NIOC Maryland
CTN1 Michelle Reed, NIOC Georgia



DIVERSITY

WOMEN'S EQUALITY DAY



WOMEN'S EQUALITY DAY HONORS ACHIEVEMENTS OF WOMEN'S RIGHTS MOVEMENT

By MC2(SW) Christopher J. Koons

Throughout American history, women have sought to gain equality with men in every sphere of life. As a result of their efforts, in 1971, Congress designated Aug. 26 as Women's Equality Day to commemorate the passage of the 19th Amendment granting women the right to vote and to celebrate continuing efforts toward equality.

The first women's rights convention in the United States was July 19-20, 1848, in Seneca Falls, NY. Lucretia Mott, Elizabeth Cady Stanton, Martha C. Wright, Mary Ann McClintock and Jane Hunt -- all of whom were involved in the fight for female and minority rights -- met with other delegates and drew up a "Declaration of Sentiments" about the status of American women.

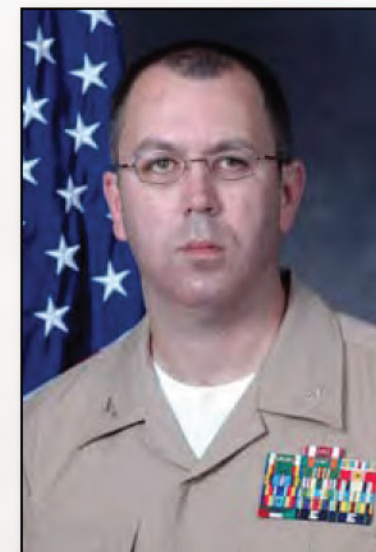
Echoing the words of the Declaration of Independence, it read that "all men and women had been created equal" and went on to list 18 "injuries and usurpations on the part of man toward woman." One of the rights it demanded for women was the right to vote.

On Aug. 26, 1920, the 19th Amendment to the Constitution was ratified. It stated: "the right of citizens of the United States

to vote shall not be denied or abridged by the United States or by any State on account of sex. Congress shall have power to enforce this article by appropriate legislation."

In the following decades, women worked to gain equality with men in employment, pay and the holding of elected office. These efforts led to passage of laws such as the Equal Pay Act of 1963, which made it illegal for employers to pay a woman less than a man for the same job, and the Civil Rights Act of 1964, which barred discrimination in employment on the basis of race and sex.

Today, workplaces and public facilities participate in Women's Equality Day with programs, displays, video showings and other activities that draw attention to the history of and continuing efforts to achieve full female equality in the United States. ♀



Society of American Indian Government Employees

CAPT Rex A. Guinn, NETWARCOM's staff judge advocate, recently received the Society of American Indian Government Employee (SAIGE) Recognition award for 2009 at the 6th annual SAIGE training conference in San Diego. Guinn was recognized for his dedication, support and promotion of the SAIGE mission. (Official U.S. Navy Photo)



UPCOMING DIVERSITY CONFERENCES

CONFERENCE	LOCATION	DATES	WEBSITE
• Sea Services Leadership Assoc. (SSLA) Symposium	Washington	18-19 Jun	www.sealeader.org
• (NAACP) Convention/Academic, Cultural, Tech Scientific Olympics	New York	11-17 Jul	www.naACP.org/youth/act-so
• League of United Latin American Citizens (LULAC) National Convention	San Juan, Puerto Rico	13-18 Jul	www.lulac.org
• Federally Employed Women (FEW) National Training Conf.	Orlando, FL	20-24 Jul	www.few.org
• National Naval Officers Assoc. (NNOA) Conference	Houston	20-24 Jul	www.nnoa.org
• Mana Hermanitas Summer Leadership Institute	Orlando, FL	23-26 Jul	www.hermana.org
• Black Data Processing Assoc. (BDPA)	Raleigh, NC	25-8 Aug	www.bdpa.org/portal
• National Tuskegee Airmen Inc. (TAI) Convention	Las Vegas	6-9 Aug	www.tuskegeearmen.org
• Blacks in Government (BIG) National Conference	Baltimore	24-28 Aug	www.bignet.org
• Historically Black Colleges & Universities (HBCU) White House Initiative Conference	Washington	30 Aug -3 Sep	www.ed.gov/whhbcu
• National Latina Style Magazine Symposium	Washington	10 Sep	www.latinastyle.com
• Academy Women 6th Annual Leadership Symposium	Arlington, VA	18-20 Sep	www.academywomen.org

EDITOR'S NOTE: For more information on NETWARCOM's Diversity Program contact: LCDR Mark A. Venzor at (757) 417-7931 X 1 or mark.a.venzor@navy.mil

DEPARTMENT OF THE NAVY

Naval Network Warfare Command
Public Affairs Office
2465 Guadalcanal Road
Norfolk, VA 23521-3228

**PRESORTED STANDARD
U.S. POSTAGE PAID
SOUTHERN MARYLAND
PERMIT No. 1968**

Address Service Requested

Official Business

